COMMITTEE OF EXPERTS ON THE EVALUATION
OF ANTI-MONEY LAUNDERING MEASURES AND
THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2021)24

# Anti-money laundering and counter-terrorist financing measures

# Croatia

## Fifth Round Mutual Evaluation Report

December 2021

**The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL** is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The fifth round mutual evaluation report on Croatia was adopted by the MONEYVAL Committee at its 62nd Plenary Session (Strasbourg, 15 December 2021).

*Contents*

# EXECUTIVE SUMMARY

1. This report provides a summary of the anti–money laundering and combating financing of terrorism (AML/CFT) measures in place in Croatia as at the date of the on–site visit (10–21 May 2021). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Croatia's AML/CFT system and provides recommendations on how the system could be strengthened.

## Key Findings

a) The understanding of money laundering (ML) risks is uneven across the Croatian authorities. The supervisors' understanding ranges from comprehensive to inadequate in the order from Croatian National Bank (CNB), Financial Inspectorate, Croatian Financial Services Supervisory Agency (CFSSA) to Tax Administration (TA). Amongst the law enforcement authorities (LEAs), the State Attorney's Office (SAO) and the Security and Intelligence Agency (SIA) level of ML risk understanding was mostly identical, and reflective of the National Risk Assessment (NRA) findings. The Anti–Money Laundering Office's (AMLO) risk understanding was broader than the NRA suggests. The Terrorist financing (TF) risks understanding did not prove to be sufficient across all authorities, with the CNB and the Financial Inspectorate demonstrating a comparably better understanding at a sectoral level. Overall, understanding of ML/TF risks was affected by several shortcomings in identification and assessment of risks. Three strategic documents, while not informed by the ML/TF risks, are developed aimed at setting policy objectives, in the areas of suppression of corruption and prevention of TF. Two Action Plans on the basis of NRAs are described by Croatia as representing a national AML/CFT policy, which raises doubts on the basis of the substance of these. At an operational level, competent authorities demonstrated good co–operation and co–ordination on ML/TF issues, but support at the policy–making level is not demonstrated enough regarding strategic coordination of combating ML/TF.

b) The competent authorities access a wide variety of sources of financial intelligence and other relevant information when conducting investigations. LEAs leverage financial intelligence mostly to develop evidence and trace criminal proceeds related to associated predicate offences. They rarely use these in the context of ML investigations and never for TF investigations (but were systematically used in TF pre–investigations led by LEAs). Suspicious transaction reports (STRs) received especially from banks and Money Value Transfer Services (MVTS) contain relevant and accurate information, which assists the AMLO and LEAs when performing their duties. LEAs acknowledge the quality of the AMLO disseminations. Most investigations are triggered by the AMLO disseminations, but the ratio between disseminated cases and launched investigations remains low. The AMLO disseminates the results of its analysis to LEAs, but in some instances (rarely with respect to ML and systematically for TF) these are addressed to authorities with no law enforcement powers. The AMLO conducts strategic analysis, however, it does not sufficiently reflect the

higher risk areas identified in the NRA. The AMLO suffers from a significant shortage of human resources, which affects its performance.

c) The legislation provides extensive powers to LEA to identify and investigate ML. However, the investigation mainly focuses on the predicate offence due to the limited understanding of ML offence by judges and to some extent prosecutors. Overall achieved results in ML convictions are not consistent with the risk profile of the country. Criminal sanctions applied so far for ML offences are not sufficiently effective or dissuasive.

d) Croatian authorities have legal powers to detect, restrain and confiscate instrumentalities, proceeds of crime and property of equivalent value. While there is no high policy document regarding confiscation, the actions of the competent authorities in recent years demonstrate that confiscation is considered a policy objective to some extent. Croatia has confiscated significant proceeds of domestic predicate offences, but ML related confiscation has not achieved any tangible results. The financial investigations are carried out as a part of the investigation of predicate offences, but authorities do not keep statistics on those and cannot provide results of the specific outcomes. Undue delays in criminal proceedings in complex cases cause the release of the seized assets and create the risk of dissipation of assets. Cross–border transportation of cash very rarely triggered ML/TF inquires by LEAs. Confiscation results are not always in line with the risk profile of the country described in both 2016 and 2020 NRAs.

e) The authorities do not have a proper understanding of TF phenomenon and how different legal and illegal activities can be exploited for TF purposes. While there were a number of inquiries conducted by LEAs, these did not lead to any formal criminal or parallel financial investigation and thus no prosecution and conviction for TF offence. While in certain instances this is due to the lack of sufficient criminal grounds, in others, it is due to the lack of consideration of TF elements in specific cases.

f) Croatia implements the UN targeted financial sanctions (TFS) on TF and proliferation financing (PF) relying on the European Union (EU) legal framework, which does not ensure implementation of those "without delay". There is no national legal framework set to overcome this delay. No national framework is also set for identifying and designating persons and entities pursuant to UNSCRs 1267/1989 and 1988 and 1373. No procedures or mechanisms for de–listing or unfreezing assets are available publicly. The Standing Group did not demonstrate an active role in implementation of asset freezing requirements in the country. Banks and other REs that are members of larger financial groups demonstrated sufficient understanding of TF and PF–related UN TFS requirements. Tools for implementation of the TFS used by the most material REs ensure timely update and effective detection of matches. Smaller REs have weaknesses in understanding some requirements related to the frequency and the scope of checks. While no real match was detected and no assets frozen, several REs confirmed having had false–positive matches with UN TFS listed persons, thus demonstrating the ability to detect matches.

Supervision of compliance with PF–related TFS is conducted within the scope of AML/CFT inspections, but there is a need for more frequent supervisory efforts focused on the weaker performing sectors, and adequate resourcing.

g) Croatia made efforts to conduct assessment of risks in the non–profit organisations (NPO) sector. The NPO sector was considered within the scope of the two NRAs conducted in 2016 (subject to ML vulnerabilities in the sector), 2020 (as a variable for assessing the Country's TF vulnerabilities), and a thematic analysis by the Financial Inspectorate. None of these exercises led to identification of the subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse by virtue of their characteristics. This has affected the implementation of the targeted measures towards the sector.

h) The level of understanding of ML risks, while in conformity with the NRA findings, varies across sectors, being stronger among banks, MVTS, and to a lesser extent among authorised exchanges, Virtual Asset Services Providers (VASPs), lawyers and notaries. With respect to TF risks, banks' and MVTS's understanding is relatively higher than across all other sectors, where understanding is deficient. Generally, where REs have a limited understanding of ML/TF risks, this directly impacts the application of risk–mitigating measures. Banks and MVTS demonstrated advanced practices in applying a risk–based approach, consistent with their risk understanding and assessment of their own businesses' risks. Financial Institutions (FIs) and designated non–financial businesses and professions (DNFBPs) exhibited different degrees in the application of customer due diligence (CDD) measures, including the depth and sophistication of ongoing monitoring of business relationships, relatively stronger being banks, MVTS, authorised exchange, and online casino providers. Implementation of CDD requirements to natural persons is adequate, but application of measures to identify beneficial owner (BO) of a corporate customer raises concerns within all sectors, especially when dealing with complex structures. FIs, especially banks, MVTS, E–money and payment institutions demonstrated a higher level of effectiveness in applying enhanced due diligence (EDD) measures than the DNFBPs. The STRs align with the risks identified in the NRA to a large extent. The volume of STRs in the banking and MVTS (including the Croatia Post) sectors is largely consistent with the expectations, taking into consideration the materiality and risks present in the sectors than that of the others. STR reporting in non–bank FIs, including exchange offices and DNFBPs, including casinos, notaries, and real estate is low and may indicate a lack of understanding of reporting requirements or inadequate controls to identify suspicious activity.

i) When licensing, the CNB applies robust measures including verification of received information, while the CFSSA does so to a lesser extent. The TA and other licensing bodies apply administrative checks without verification of a criminal background information. The CNB and Financial Inspectorate have a reasonable supervisory framework with their AML/CFT supervisory efforts largely aligned to understanding the ML/TF risks. The shortcomings of risk understanding by the CFSSA and the TA also impact the effectiveness of the

supervision undertaken. The effectiveness and dissuasiveness of sanctions vary across the supervisors, being stronger at the CNB and Financial Inspectorate whilst weaker at the CFSSA and the TA.

j) Information on the creation and types of legal persons and arrangements is publicly accessible. While no assessment was conducted, the authorities, independent of each other, demonstrated some understanding of ML but not TF vulnerabilities of legal persons and arrangements. While observing that limited liability companies and Simple limited liability companies are the types of legal persons most frequently abused, Croatian authorities are reluctant to flag certain types of legal persons as the most vulnerable vehicle for ML, rather, they are inclined to focus on the schemes and criminal conduct itself. There is a range of measures to mitigate the misuse of legal persons and arrangements, such as the requirement to register in various registers, including the BO Register, participation of a notary public in the registration process, but all of these have some weaknesses. Issues with verification of information and ongoing monitoring undermine the accuracy of the information and how up to date it is. Adequacy of information casts doubts in some instances. Access to information and documents by competent authorities is timely. Sanctions are not applied in a systematic manner.

k) Croatia provides constructive assistance in the field of MLA and extradition in relation to ML/TF, and predicate offences (except for the fiscal offences when dealing with non–EU Member States). There are no major issues in international co–operation, but occasional delays are observed when requests are sent through the MoJA. There is no mechanism for prioritising incoming requests. Croatia is seeking foreign co–operation only to a limited extent, which is not in line with its risk profile. The country has not taken a systematic approach to identify and eliminate the underlying systemic issues with refusing extradition requests by foreign counterparts. Informal co–operation represents a strong side of the system.

## Risks and General Situation

2. The main ML risks detected by Croatia are related to tax crime, corruption and drug trafficking. Among these, tax crime and drug trafficking are not only posing domestic risks but also foreign. Setting up legal persons by non–residents and seeking to transfer funds to or through Croatia's financial system is a well–known typology. Croatia takes measures towards preventing this risk. Croatia is a transit point along the so called "Balkan route" through which narcotics are smuggled to Western Europe, by organised criminal groups. Corruption is mostly detected as a domestic crime. A number of criminal proceedings against high–ranking public officials, including the former prime minister were carried out. Modalities of such illegal behaviour include budget payments for unperformed or unreasonably high marketing and similar services. Croatia considered the terrorism threat to be low in the country, with very few instances of Croatian nationals leaving for conflict zones.

## Overall Level of Compliance and Effectiveness

3. Croatia introduced major amendments into its Anti–Money Laundering and Terrorism Financing Law (AMLTFL) in 2018 and subsequently in 2019, considerably enhancing the requirements for application of preventative measures. It also has conducted two NRAs in 2016 and 2020 respectively. The findings of the first NRA led to application of enhanced measures for the identification of a customer. Croatia also took important steps towards improving transparency of legal persons and arrangements by introducing a BO Register. First steps were also taken towards introducing the VASPs into the AML/CFT framework, setting a requirement for VASPs to file a notification to CFSSA about their activities.

4. In terms of technical compliance, the legal framework has been significantly amended, but a number of technical shortcomings are noted some of which present challenges for effectiveness. There are gaps with implementation of UN TFS on TF and PF, measures with respect to the NPO sector, certain preventive measures related to the implementation of CDD. Some of the challenges related to inadequate resourcing of competent authorities had a systematic impact. This speaks to a need for more support at a policy level. Croatia demonstrated strengths in implementation measures related to financial institutions secrecy laws, analysis function of the FIU, deployment of competent authorities with law enforcement responsibilities, and providing guidance and feedback across the private sectors.

*Assessment of risk, coordination, and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)*

5. Croatia has made efforts to develop its understanding of ML/TF risks through two NRAs conducted in 2016 and 2020. The second NRA does not demonstrate an increased level of understanding from the first one, and it did not lead to a more sophisticated understanding and response to ML/TF risks. The understanding of ML risks is uneven across the Croatian authorities. The supervisors' understanding ranges from comprehensive to inadequate in the order from CNB, Financial Inspectorate, CFSSA to TA. Amongst the LEAs, the SAO and the SIA level of ML risk understanding was mostly identical and reflective of the NRA findings. The AMLO's risk understanding was broader than the NRA suggests regarding observed trends and typologies. The TF risks understanding did not prove to be sufficient across all authorities, with the CNB and the Financial Inspectorate demonstrating a comparably better understanding at a sectoral level.

6. Overall, understanding of ML/TF risks was affected by several shortcomings in identification and assessment of risks: conclusions are based on the empirical knowledge due to the systemic lack of quantitative data; data on undetected criminality is not explored; STRs and other financial intelligence and a range of foreign co–operation requests are not systematically explored. The authorities could mainly describe the top three ML threats in terms of the predicate offences but could not explain them in terms of the ML risks. The impact of certain vulnerabilities on the risk environment of the country was not demonstrated to be understood.

7. Three strategic documents, while not informed by the ML/TF risks, are developed aimed at setting policy objectives, in the areas of suppression of corruption and prevention of TF. Two Action Plans on the basis of NRAs are described by Croatia as representing a national AML/CFT policy, which raises doubts on the basis of the substance of these.

8. At an operational level, competent authorities demonstrated good co–operation and co–ordination on ML/TF issues, but support at the policy–making level is not demonstrated enough regarding strategic coordination of combating ML/TF.

*Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)*

9. The competent authorities access a wide variety of sources of financial intelligence and other relevant information when conducting investigations. LEAs leverage financial intelligence mostly to develop evidence and trace criminal proceeds related to associated predicate offences. They rarely use these in the context of ML investigations, and never for TF investigations (but were systematically used in TF pre–investigations led by LEAs). LEAs co–operate with the AMLO to obtain relevant financial intelligence in the framework of their investigations. STRs are generally of good quality and, despite an apparent lack of human resources, the AMLO produces valuable operational analysis. LEAs acknowledge the quality of the AMLO disseminations; however, the ratio between these and launched investigations remains low, and mainly focuses on predicate offences. In addition, LEAs do not provide sufficient feedback to the AMLO as regards the outcome and the quality of its disseminations. The AMLO does not proactively request information from competent authorities to enrich its cases. Although the AMLO conducts strategic analysis, it is limited and does not sufficiently reflect on higher risk areas. Neither does the AMLO provide targeted, and as required a case–by–case feedback to REs on their reporting.

10. Croatia has extensive legal powers enabling identification and investigation of ML. However, the ML is not prioritised as a national policy objective. ML cases are mainly triggered by the AMLO dissemination, and only a few investigations have been triggered by performance of LEAs. It is noticeable that there is a general lack of comprehensive understanding of the ML offence by the judges and to some extent, by prosecutors. Namely, it is a common understanding, as well as an opinion expressed in the Supreme Court jurisprudence that depositing the proceeds of crime in the bank account of different natural persons is the only safe way to store money before its further usage. In addition, cumulative execution of all stages of ML (placement, layering and integration) is required. This affects identification of ML offence by LEAs, and when identified, the high evidentiary threshold for ML offence usually cause authorities to transfer the case to third countries where the predicate crime occurred.

11. There is a sound legal framework in Croatia on freezing, seizing and confiscation of instrumentalities and proceeds of crimes, confiscation of equivalent value, as well as extended confiscation. Confiscation of proceeds, instrumentalities and equivalent value is pursued as a policy objective in Croatia to some extent. The effectiveness of the confiscation in relation to the domestic proceeds generating predicate offences has been achieved to some extent. No significant proceeds of ML offence have been seized or confiscated. Regarding TF, there have been no seizure or confiscation, since Croatia did not investigate or prosecute any TF cases. Cross border cash controls rarely triggered any ML investigation, and administrative sanctions applied are considered not to be dissuasive. The confiscation results achieved so far do not appear to be fully consistent with the level of ML/TF threat present in the country and national AML/CFT policies and priorities.

*Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)*

12. Croatia's legal framework to fight TF is in line with international standards to a large extent. There have been no TF prosecution or conviction in Croatia so far. The authorities did not demonstrate a proper understanding of the TF phenomenon and how different legal and illegal activities can be exploited for TF purposes. There have been no TF investigations, and neither was a proactive approach concerning TF identification demonstrated. The authorities have detected some potential cases of TF, and only preliminary inquiries have been undertaken concerning TF.

However, authorities did not demonstrate that they have undertaken appropriate steps to properly detect TF even though the evaluators came across several examples where potential TF activities should have been at least considered for investigation.

13. Croatia implements the UN TFS on TF and PF relying on the EU framework, which does not ensure implementation of those "without delay". There is no national legal framework set to overcome this delay. No national framework is also set for identifying and designating persons and entities pursuant to UNSCRs 1267/1989 and 1988 and 1373. No procedures or mechanisms for de–listing or unfreezing assets are available publicly. The Standing Group did not demonstrate an active role in implementation of asset freezing requirements in the country. The Ministry of Foreign and European Affairs (MFEA) does not demonstrate actively performing its role in implementation of the UN TFS. Banks and other REs that are members of larger financial groups demonstrated sufficient understanding of TF and PF–related UN TFS requirements. Tools for implementation of the TFS used by the most material REs ensure timely update and effective detection of matches. Smaller REs have weaknesses in understanding some requirements related to the frequency and the scope of checks. While no real match was detected and no assets frozen, several REs confirmed having had false–positive matches with UN TFS listed persons, thus demonstrating the ability to detect matches. Supervision of compliance with PF–related TFS is conducted within the scope of AML/CFT inspections, but there is a need for more frequent supervisory efforts focused on the weaker performing sectors and adequate resourcing.

14. Croatia made efforts to conduct risk assessment in the NPO sector. The NPO sector was considered within the scope of the two NRAs conducted in 2016 (subject to ML vulnerabilities in the sector), 2020 (as a variable for assessing the Country's TF vulnerabilities), and a thematic analysis by the Financial Inspectorate. None of these exercises lead to identification of the subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse by virtue of their characteristics. This has affected the implementation of the targeted measures towards the sector.

*Preventive measures (Chapter 5; IO.4; R.9–23)*

15. The level of understanding of ML risks, while in conformity with the NRA findings, varies across sectors, being stronger among banks, MVTS, and to a lesser extent among authorised exchange operators, VASPs, lawyers and notaries. Other FIs, and casinos are aware of the NRA findings, but similarly to the rest of the sectors they could not always explain their risk exposure, in practice. With respect to TF risks, banks and MVTS's understanding is relatively higher than across all other sectors, where understanding is deficient. Overall, all REs could explain their AML/CFT obligations, where FIs could display clear understanding, VASPs – acceptable level, and the DNFBPs – varied, but mostly being at a basic level.

16. Where REs have a limited understanding of ML/TF risks, this has a direct impact on the application of risk–mitigating measures. Banks and MVTS demonstrated advanced practices in applying a risk–based approach, consistent with their risk understanding and assessment of their own businesses' risks. Authorised exchanges, lawyers and notaries demonstrated the development of their own risk indicators, and casinos, demonstrated the application of additional risk mitigation measures to online gambling services. The majority of other FIs and DNFBPs apply mitigating risks uniformly, without tailoring to their risk characteristics. FIs and DNFBPs exhibited different degrees in application of CDD measures, including the depth and sophistication of ongoing monitoring of business relationships. Relatively stronger performing sectors are banking, MVTS, authorised exchange, and online casino providers. Implementation of

CDD requirements to natural persons is adequate, but application of measures to identify BO of a corporate customer raises concerns within all sectors, especially when dealing with complex structures. FIs, especially banks, MVTS, E–money and Payment Institutions demonstrated a higher level of effectiveness in applying EDD measures than the DNFBPs. The application of EDD measures by REs is not always proportionate to the level of observed risks, but rather is applied to meet the legislative obligation only. The STRs align with the risks identified in the NRA to a large extent. The volume of STRs in the banking and MVTS (including the Croatia Post) sectors is largely consistent with the expectations, taking into consideration the materiality and risks present in the sectors than that of the others. STR reporting in non–bank FIs, including authorised exchanges and DNFBPs, including casinos, notaries, and real estate is low and may indicate a lack of understanding of reporting requirements or inadequate controls to identify suspicious activity.

*Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)*

17. All the licensing authorities and SRBs have in place legislative requirements on the prevention of criminals from holding a management function or being the BO of a REs, but among those the CNB applies robust measures including verification of received information, while the CFSSA does so to a lesser extent. The TA and other licensing bodies apply administrative checks without verifying criminal background information. All FIs and DNFBPs are covered by licensing and registration requirements, except for newly regulated VASP sector, where notification mechanism is introduced and some less material DNFBPs (accountants, TCSPs and dealers in precious metals and stones (DPMS)). The CNB and Financial Inspectorate have a reasonable supervisory framework, and their AML/CFT supervisory efforts are largely aligned to their understanding of the ML/TF risks. The shortcomings of risk understanding by the CFSSA and the TA also impact the effectiveness of the supervision undertaken. In 2020 the CNB revised its supervisory cycles, and the approach which is expected to make the process more risk–oriented, and resource optimised. The supervisory efforts of the Financial Inspectorate are impacted by the shortage of resources and the available IT support. This led to a decrease in on–site and an increase in off–site supervision. Nonetheless this has not affected the overall quality and effectiveness of the supervisory regime. Performance in terms of implementation of AML/CFT supervisory measures are weaker at CFSSA and to a larger extent at the TA, which are responsible for less material sectors. The effectiveness and dissuasiveness of sanctions vary across the supervisors, being stronger at the CNB and Financial Inspectorate, whilst weaker at the CFSSA and TA. Whilst monetary sanctions are imposed through the Council of Misdemeanour Proceedings these are not deemed effective or dissuasive for some sectors, such as Banks.

*Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)*

18. Information on the creation and types of legal persons and arrangements is publicly accessible. While no assessment was conducted the authorities independently of each other demonstrated some understanding of ML but not TF vulnerabilities of legal persons and arrangements. While observing that the limited liability companies (LLC) and Simple LLCs (SLLC) are the types of legal persons that are most frequently abused, Croatian authorities are reluctant to flag certain types of legal persons as the most vulnerable vehicle for ML, rather, they are inclined to focus on the schemes and criminal conduct itself. There is a range of measures to mitigate the misuse of legal persons and arrangements, such as the requirement to register in various registers, including the BO Register, participation of a Public Notary in the registration process, but all of these have some weaknesses. Access to information and documents by competent authorities is timely, but issues with verification of information and ongoing

monitoring undermine the accuracy of the information and how up to date it is. Adequacy of information casts doubts in some instances. Sanctions are not applied in a systematic manner.

*International co–operation (Chapter 8; IO.2; R.36–40)*

19. Croatia provides constructive assistance in the field of MLA and extradition in relation to ML/TF, and predicate offences (except for the fiscal offences when dealing with non–EU Member States). There are no major issues in international co–operation, but occasional delays are observed when requests are sent through the MoJA. There is no mechanism for prioritising incoming requests. Croatia is seeking foreign co–operation to a limited extent only. This approach might lead the country to miss opportunities for identifying and investigating relevant cases. Throughout the whole reporting period, the outgoing requests on freezing and confiscation of assets remained modest, which is inconsistent with Croatia's geographical exposure to ML and predicate offences. The country has not taken a systematic approach to identifying and eliminating the underlying systemic issues with refusing extradition requests by foreign counterparts. In practice, informal co–operation represents a strong side of the system. The supervisory authorities also demonstrated a relatively good level of international co–operation.

## Priority Actions

a) Croatia should strengthen its high–level policy coordination in combating ML and TF by: (i) introducing policymakers into the AML/CFT coordination mechanism – Inter–Interinstitutional Working Group for the Prevention of ML/TF (IIWG); (ii) articulating the national AML/CFT policies, objectives and activities in a strategic framework, and providing with necessary resources (budgetary and human); (iii) providing the IIWG with necessary powers for implementation of AML/CFT policies, objectives and activities commensurate to ML/TF risks; (iv) ensuring regular monitoring of the implementation of respective AML/CFT policies, objectives and activities by the IIWG, and assessment of the impact on the ML/TF risks in Croatia.

b) Croatia should enhance its ML/TF risk understanding, deepening it in the areas currently covered in the NRA and further expanding identification and assessment of risks related to ML (organised crime, use of cash cross–border risks, trade–based ML, risks related to VA and VASPs) and TF (OCG, migrant smuggling, remaining stock of weapons, financing of the FTF family members). Croatia should identify, assess and understand vulnerabilities of legal persons and arrangements, and the potential for their ML/TF abuse, and vulnerabilities of the NPO sector for the TF abuse. Croatia should ensure the use of comprehensive quantitative data (actual crime, undetected criminality, STRs, other financial intelligence, foreign co–operation requests, including MLA and other forms of co–operation), in addition to its empirical knowledge.

c) Croatia should seek to ensure that judiciary and LEAs interpretations and understanding of the ML offence are aligned with the international standards, including by: (i) developing formal guidelines drawing on international and domestic requirements for ML offence and good practices for investigating and prosecuting ML offence; (ii) promoting evolving jurisprudence on ML cases in line with the current criminalisation of ML and international standards; and (iii) holding regular

trainings.

d) Croatia should: (i) conduct analysis of all cases where preliminary inquiries took place to detect potential challenges in pursuing TF investigations/prosecutions; (ii) proactively coordinate between the LEAs and SAO (setting agreement or MoU where necessary) to ensure all potential TF activities are identified, thoroughly analysed, investigated and prosecuted; (iii) develop a guideline drawing on international best practices on TF investigations and prosecutions, setting out the range of circumstances and sources of information (including MLA, EAW and other incoming data) to trigger TF investigations, and (iv) provide trainings to LEAs and judiciary.

e) Croatia should clearly establish confiscation of criminal proceeds, instrumentalities and property of equivalent value as a high–level policy objective. There should be specific actions aimed at tracing and securing direct/indirect proceeds, as well as foreign proceeds for confiscation purposes. The results achieved should be commensurate with the ML/TF risk of Croatia.

f) Croatia should ensure that the AMLO is provided with adequate human resources. The AMLO should ensure that its cases are disseminated primarily to competent authorities with law enforcement powers, including by amending and further elaborating its dissemination procedures. The AMLO should: (i) provide more frequent, including as required, case–by–case feedback to REs on the outcomes and the quality of STRs; (ii) provide targeted guidance and training to REs on timely reporting of STRs.

g) Croatia should introduce mechanisms to ensure: (i) verification of all information provided at the stage of registration of a legal person; (ii) prevention criminals (ML, predicate offences and TF) from acting as a shareholder, BO, or manager of legal person, introducing a requirement for verification of criminal background of these persons, including implementation of the UN TFS measures; (iii) introduction of an ongoing monitoring mechanism for ensuring timely detection and registration of changes to basic and BO information, (iv) implementation of a mechanism for supervision to ensure the accuracy and timely update of information; and (v) imposition of effective, proportionate and dissuasive sanctions for failure to comply with the information requirements, and compiling and maintain statistics on application of sanctions. This should be followed by the assignment of clear responsibilities for authorities with supervisory function, allocation of adequate resources, and regular supervision.

h) Croatia should establish a national framework for implementation of TF and PF–related UN TFS measures without delay.

i) Croatia should establish: (i) clear mechanism or channel, and develop a reporting form, for submitting reports to MFEA on frozen assets or actions taken in compliance with the prohibition requirements, including attempted transactions by REs in line with the respective UNSCRs; and (ii) determine the recipient of these disclosures (contact point). Ensure that the MFEA's responsible recipient of disclosures has knowledge, powers and instructions for taking action upon the receipt of the disclosure from a RE. Ensure that all REs are made aware of information on reporting form, contact point and reporting channels, including that this information is publicly available.

j) Croatia should provide all supervisory authorities with the required human resources to ensure these are adequate to permit supervisory authorities to fulfil their obligations. All authorities with licensing and registration responsibilities should implement effective tools, for the identification of unauthorised operators (including where authorisation is withdrawn or surrendered) that offer (or advertise) regulated activities and conduct systematic monitoring of the market. The CNB should continue and the CFSSA should enhance its efforts in applying robust market entry measures. Other licensing and registration bodies should introduce effective measures for preventing criminals and their associates from holding or being the BO of a significant or controlling interest or holding a management function when granting authorisation.

k) Croatia should support REs (FIs, DNFBPs and VASPs) to further deepen their understanding of ML risks and develop the TF risk understanding, including also through providing the CTF guidance and training to all REs with a focus on sector–specific TF risks. Croatia should ensure that REs improve their firm–specific business risk assessments, improve implementation of CDD and EDD measures, and increase the STR reporting (especially in low/non – reporting sectors).

l) Croatia should introduce as a policy objective systematically seeking international co–operation when investigating criminal cases of ML, associated predicate offences or TF with a foreign element. Particular attention should be given to freezing, seizure and confiscation of assets moved abroad in all relevant cases. Croatia should analyse cases of refusal of its outgoing requests, taking appropriate actions to identify and eliminate the systemic issues that prevent constructive international co–operation.

## Effectiveness & Technical Compliance Ratings

### *Effectiveness Ratings*[1]

| IO.1 – Risk, policy and coordination | IO.2 – International co–operation | IO.3 – Supervision | IO.4 – Preventive measures | IO.5 – Legal persons and arrangements | IO.6 – Financial intelligence |
|---|---|---|---|---|---|
| Moderate | Substantial | Moderate | Moderate | Moderate | Moderate |
| **IO.7 – ML investigation & prosecution** | **IO.8 – Confiscation** | **IO.9 – TF investigation & prosecution** | **IO.10 – TF preventive measures & financial sanctions** | **IO.11 – PF financial sanctions** | |
| Low | Moderate | Moderate | Low | Moderate | |

### *Technical Compliance Ratings*[2]

| R.1 – assessing risk & applying risk–based approach | R.2 – national co–operation and coordination | R.3 – money laundering offence | R.4 – confiscation & provisional measures | R.5 – terrorist financing offence | R.6 – targeted financial sanctions – terrorism & terrorist financing |
|---|---|---|---|---|---|
| PC | PC | LC | LC | LC | PC |
| **R.7– targeted financial sanctions – proliferation** | **R.8 –non–profit organisations** | **R.9 – financial institution secrecy laws** | **R.10 – Customer due diligence** | **R.11 – Record keeping** | **R.12 – Politically exposed persons** |
| PC | PC | C | PC | LC | LC |
| **R.13 – Correspondent banking** | **R.14 – Money or value transfer services** | **R.15 – New technologies** | **R.16 – Wire transfers** | **R.17 – Reliance on third parties** | **R.18 – Internal controls and foreign branches and subsidiaries** |
| PC | LC | PC | LC | PC | PC |
| **R.19 – Higher–risk countries** | **R.20 – Reporting of suspicious transactions** | **R.21 – Tipping–off and confidentiality** | **R.22 – DNFBPs: Customer due diligence** | **R.23 – DNFBPs: Other measures** | **R.24 – Transparency & BO of legal persons** |
| LC | LC | LC | PC | PC | PC |
| **R.25 – Transparency & BO of legal arrangements** | **R.26 – Regulation and supervision of financial institutions** | **R.27 – Powers of supervision** | **R.28 – Regulation and supervision of DNFBPs** | **R.29 – Financial intelligence units** | **R.30 – Responsibilities of law enforcement and investigative authorities** |
| LC | LC | LC | LC | C | C |
| **R.31 – Powers of law enforcement and investigative authorities** | **R.32 – Cash couriers** | **R.33 – Statistics** | **R.34 – Guidance and feedback** | **R.35 – Sanctions** | **R.36 – International instruments** |
| LC | PC | PC | C | PC | PC |
| **R.37 – Mutual legal assistance** | **R.38 – Mutual legal assistance: freezing and confiscation** | **R.39 – Extradition** | **R.40 – Other forms of international co–operation** | | |
| LC | PC | LC | PC | | |

[1] Effectiveness ratings can be either a High– HE, Substantial– SE, Moderate– ME, or Low – LE, level of effectiveness.
[2] Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non–compliant.

# MUTUAL EVALUATION REPORT

## Preface

1. This report summarises the AML/CFT measures in place as at the date of the on–site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.

2. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on–site visit to the country from 10 to 21 May 2021.

3. The evaluation was conducted by an assessment team consisting of:

Assessors:

Ms Katherine Berry – Senior Adviser, Policy, Financial Services Commission, Jersey (financial expert)

Ms Annette Perales – Head of AML/CFT Supervision, Financial Services Commission, Gibraltar (financial expert)

Ms Elizaveta Churilina – Head of Unit, International co–operation department, Federal Financial Monitoring Service, Russian Federation (law enforcement expert)

Mr Borja Aguado Delgado – Deputy, General Prosecutor's Office, Andorra (legal expert)

Ms Maria Galstyan – Methodologist, Legal Advisor, Legal Compliance Division, Financial Monitoring Centre, Central Bank of Armenia, Republic of Armenia (legal expert)

MONEYVAL Secretariat:

Ms Ani Melkonyan – Administrator

Ms Ana Boskovic – Administrator

Ms Ariane Schneider – Project Officer

4. The report was reviewed by Ms Suzie White, Director, Mutual Evaluations Asia/Pacific Group on Money Laundering, Mr Hamish Armstrong, Chief Advisor of Financial Crime, Financial Services Commission, Jersey and the FATF Secretariat.

5. Croatia previously underwent a MONEYVAL Mutual Evaluation in 2013, conducted according to the 2004 FATF Methodology. The 2013 evaluation and 2019 exit follow–up report have been published and is available at https://www.coe.int/en/web/moneyval/jurisdictions/croatia.

6. That Mutual Evaluation concluded that the country was compliant with 7 Recommendations; largely compliant with 25; partially compliant with 16; and one Recommendation was non–applicable. Croatia was rated compliant or largely compliant with 9 out of 16 Core and Key Recommendations.

7. Following the adoption of the 4th Round MER, Croatia was placed under the regular follow–up procedure. In July 2019, Croatia exited the follow–up process on the basis that it had reached a satisfactory level of compliance with most of the Core and Key Recommendations, and that the Plenary used the limited flexibility provided by Rule 13, para. 4 of the Rules of Procedures to remove Croatia from the 4th round follow–up process.

# 1. ML/TF RISKS AND CONTEXT

1. Croatia is situated in the south–eastern part of Europe, surrounded by the Alps in the west, Sava and Drava rivers in the north and east and the Adriatic Sea in the south, with a land area of 56 594 square kilometres. According to the mid–2019 population estimate, Croatia has 4 065 253 inhabitants3. In 2020 Gross Domestic Product (GDP) amounted approximately EUR 47.27bn[4]. Croatia borders Slovenia, Hungary, Serbia, Bosnia and Herzegovina, Montenegro and shares a maritime border with Italy. Zagreb is the capital city and political, administrative and economic centre. Croatia has 21 counties, 128 cities and 428 municipalities.

2. Croatia is an independent sovereign Republic with a parliamentary form of government. The government structure is based on the separation of legislative, executive and judicial powers. The Parliament is vested with legislative power consisting of a minimum of 100 and a maximum of 160 members, elected for a term of four years. Currently, the Parliament has 151 members who were elected on 5 July 2020. The Parliament is chaired by the Speaker of the Parliament. The Government exercises executive power, which is formed by a majority vote of confidence by the Members of the Parliament. The Prime Minister is the head of the Government and appointed by the President of the Republic, and the decision is co–signed by the Speaker of the Croatian Parliament. The Parliament supervises the work of the Government in conformity with the Constitution and laws. The President of the Republic is elected for a term of five years and entrusted to ensure the regular and balanced functioning and stability of state authority.

3. Judicial power in Croatia is administered by the independent judiciary comprised of the Supreme Court, County courts and Municipal courts. There are also specialised courts operating in Croatia, such as commercial courts, administrative courts, misdemeanour courts, the High Commercial Court, the High Administrative Court and the High Misdemeanour Court. The judges are required to be impartial and are independent of the other branches of government.

4. Croatia's legal system is based on a civil law principle. Primary legislation is in the form of laws and secondary in the form of regulations. International agreements require ratification by Parliament. The Constitution stipulates that obligations imposed under ratified international treaties prevail over domestic law.

5. Croatia entered the European Union (EU) in 2013. It is not a signatory of the Schengen Agreement. The national currency is Kuna (HRK)[5]. Croatian Kuna was included in the Exchange Rate Mechanism (ERM II) in July 2020. The agreement on the participation of the Kuna in ERM II is based, inter alia, on the commitment by Croatia to join the Banking Union and ERM II simultaneously and the completion by the Croatian authorities of a set of measures described in the Croatian letter of intent dated 4 July 2019[6]. These measures pertain to the following six policy areas: banking supervision, the macro–prudential framework, the anti–money laundering framework, the collection, production and dissemination of statistics, public sector governance and the reduction of the financial and administrative burden on the economy.

6. Croatia is a member of numerous international organisations, including the Egmont Group, the United Nations (UN), the Council of Europe (COE), the Organisation for Security and Co–operation

[3] The Croatian Bureau of Statistics: https://www.dzs.hr/
[4] https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=HR&name_desc=false
[5] For the purpose of this report the exchange rate used is EUR 1= HRK 7.5, and amounts are rounded.
[6] https://www.hnb.hr/en/–/republika–hrvatska–uputila–pismo–namjere–o–ulasku–u–europski–tecajni–mehanizam–erm2–

in Europe (OSCE), the World Trade Organisation (WTO), the European Bank for Reconstruction and Development (EBRD), the World Bank, the International Monetary Fund (IMF), the Organisation for Economic Co–operation and Development (OECD), and International Police (INTERPOL).

## 1.1. ML/TF Risks and Scoping of Higher Risk Issues

### *1.1.1. Overview of ML/TF Risks*

7. Croatia faces ML threats from proceeds of crime generated both domestically and internationally, particularly through the use of its financial, property, retail sectors and legal entities. The offences that are estimated as posing a high ML threat (committed most frequently and generate considerable proceeds of crime) are tax evasion (tax or customs duty evasion), drug crime (unauthorised production and trade in illicit drugs, enabling the use of illicit drugs), and corruption (accepting bribes, giving bribes to elected representatives, accepting bribes in business dealings, trading in influence, abuse of trust in economic business, abuse of position and authority)[7].

8. Croatia is vulnerable to ML risks from neighbouring countries. It is exposed to cross–border illicit flows (related to crimes in other countries), including any significant potential role as a transit route for illicit goods or funds transfers. Use of financial and real estate sectors, abuse of professional services and companies, and use of cash in ML–related schemes with the involvement of foreign nationals are identified as long–standing patterns. Typically, the foreign criminals seek to move funds through the Croatian financial system, setting up legal entities with no apparent economic activities, withdrawing funds in cash, transferring abroad or investing in Croatian real estate. This exposes Croatia to potential cross–border ML threats, including proceeds from tax evasion, drug trafficking, fraud, trafficking in human beings and human smuggling, organised crime and other crime entering the Croatian market from abroad.

9. Organised criminal groups ("criminal associations") are active in Croatia. They feature in the three offences posing high ML threat and other offences, estimated as posing medium ML threat, such as fraud, abuse of intellectual property rights, avoidance of customs control, trafficking in human beings and human smuggling, prostitution, embezzlement and usury[8]. Several criminal associations were indicted over the last years for tax evasion, drug trafficking and corruption reducing organised crime in Croatia. Most prominently, organised crime groups are present in drug trafficking–related crimes. Croatia is a transit point along the so called "Balkan route" through which narcotics are smuggled to Western Europe. It is also used as a transit point for maritime shipments of South American cocaine bound for Western Europe[9]. In one case, in co–operation with other partners, authorities confiscated over a ton of cocaine worth around EUR18 million (mln.) (and other assets and cash estimated value of EUR3 mln.), in several countries, including Croatia. Croatia has indicated that in 2018, ten criminal associations were indicted that dealt with drug trafficking (30.3% of all criminal associations reported). Between 2013 and 2015, these criminal associations accounted for the majority of criminal associations (2015–45.8%,

[7] NRA 2016, p. 17–18, NRA 2020, p.5.
[8] Idem.
[9] https://www.occrp.org/en/daily/14234–officials–say–croatian–port–appears–to–be–new–entry–point–for–drugs https://www.policija.si/eng/newsroom/news–archive/95619–the–slovenian–criminal–investigators–apprehended–one–of–the–organisers–of–transports–of–cocaine–from–panama–to–europe–2018

2014–40.00%, 2013–46.7%), only to be followed by a decline to 26.7% in 2016 and 10.5% in 2017[10].

10. According to the Transparency International's Corruption Perception Index (CPI) Croatia is scored 47/100[11], which is a lower level compared to other western European and EU Member States. According to the European Commission surveys' results, "perceived corruption" in Croatia is higher than the EU average[12]. Significant cases relating to corruption were launched by the State Attorney's Office (SAO), and a number of criminal proceedings against high–ranking public officials, including the former prime minister[13], several heads of regional and local self–government units and public authorities, directors of state–owned entities, are pending before Croatian courts. Modalities of such illegal behaviour include budget payments for unperformed or unreasonably high marketing and similar services, purchase of real estate for public authorities at unrealistically high prices based on false estimates, sale of strategically important companies, concessions, and other public property to private entities for bribes or at unrealistically low prices or giving loans without prescribed means of payment security[14]. Croatia estimates that on an annual basis, the volume of proceeds from corruption exceeds EUR 200 mln.[15]. Use of cash and internet banking services in corruption schemes is highlighted by the authorities as a common pattern[16].

11. Croatia currently faces a low domestic terrorism threat. There have been no investigations, prosecutions or convictions for terrorism in Croatia. In 2014, one person was convicted of a criminal offence related to terrorism. One of the terrorism risks that authorities have highlighted is the remaining stock of weapons in Croatia. Authorities also acknowledge external threats, such as illegal migration and radicalisation of individuals in neighbouring Western Balkan countries. Nevertheless, there have been 7 Croatian nationals identified travelling (6 with dual nationality and 1 with single nationality) to conflict zones such as Syria and Iraq (see IO.9). This points out the potential presence of terrorism financing threat in Croatia. Croatia estimated its TF risk at the level of medium low[17] in 2016 NRA. This, however, was consequently revised by the authorities, concluding that the TF risks were reduced to low in the 2020 NRA[18]. NRA and discussions with authorities did not reveal the consistent reasoning behind either assessment.

12. Croatia identified no financial or DNFBP sector as having a high level of vulnerability. The money or value transfer services (MVTS), accountants and dealers in precious metals and stones (DPMS) sectors are assessed as posing a higher (medium–high) vulnerability for ML. Vulnerabilities in the MVTS sector are related to a predominant use of these services for cross–border money remittances, weaknesses in the implementation of the AML/CFT measures and frequent use of these services for transfer of illicit proceeds. Vulnerabilities in the sector of accountancy services are related to the lack of the market entry regulatory framework (fit and proper checks), weaknesses in the implementation of the AML/CFT measures and STR reporting, possibilities of using the business/profession in fraud or tax evasion schemes and providing TCSP

[10] Annual report on the work of state attorney's offices in 2018
[11] https://www.transparency.org/en/cpi/2020/index/hrv
[12] Special Eurobarometer 470, Corruption, Flash Eurobarometer 457, Businesses' Attitudes Towards Corruption in the EU
[13] https://kyc360.riskscreen.com/news/ex–croatia–pm–jailed–after–court–ups–his–corruption–sentence/
[14] NRA 2020, p.12
[15] NRA 2016, p.26
[16] NRA 2020, p.13
[17] NRA 2016, p.183
[18] NRA 2020, p.268

services. In addition, vulnerabilities within DPMS are related to the lack of the market entry regulatory framework (fit and proper checks), weaknesses in the implementation of the AML/CFT measures, possibilities of using the business/profession in fraud schemes.

13. The VASP sector is newly developing. Since 2020, the VASP is designated as a RE in Croatia. Banks and other financial institutions do not provide VASP services. The vulnerabilities in the VASP sector are assessed as being at a medium level due to the important regulatory gaps in the system. There is no accurate knowledge of the market size yet, due to the recent nature of regulatory requirements, but 15 VASPs are already registered with the CFSSA in Croatia[19]. The authority's estimation of the annual volume of transactions conducted by VASPs in 2020 amounts to EUR 62 037 799[20]. Over 60% of transactions are estimated to be conducted by natural persons residing in Croatia[21]. Despite the market is new and developing, the VASPs operating in the market detected attempts to use these services for fraudulent activities and by organised criminal groups.

### *1.1.2. Country's Risk Assessment & Scoping of Higher Risk Issues*

14. Croatia conducted two NRAs with reports adopted by the Government and published respectively in 2016 and 2020. The NRA was coordinated by the Inter–institutional Working Group on Money Laundering and Terrorist Financing (IIWG), consisting of 11 institutions involved in the anti–money laundering and terrorist financing (AML/CFT) activities (AMLO, SAO, Ministry of Interior (MoI), Financial Inspectorate, TA, Customs Administration (CA), Croatian National Bank (CNB), Croatian Financial Services Supervisory Agency (CFSSA), Security and Intelligence Agency (SIA), Ministry of Justice an Administration (MoJA) and Ministry of Foreign and European Affairs (MFEA)), with participation of representatives of the private sectors (either directly, or by submission of information). In both assessments, Croatia used the World Bank's National ML and TF risk assessment tool, and the work was influenced by the EU supra–national risk assessment. The first assessment was conducted with technical support of the WB[22], and the second without it.

15. The NRAs analyse both the ML and TF risks. Croatia identifies major threats, ML/TF risk enhancing and reducing factors, and provides a final residual risk rating (i.e., taking into account AML/CFT measures in place) to financial and non–financial sectors operating in the country.

16. As further explored under Immediate Outcome 1, the NRA is a good starting point for expressing ML/TF threats and vulnerabilities at a national level. However, there are noticeable deficiencies in grouping various types of entities under the same category, scoring vulnerabilities in these sectors, and limitations in some of the information used for the analysis, both qualitative and quantitative. Some sectorial risk assessments have been made by the supervisory authorities, which contain improved analysis on vulnerabilities.

17. Croatia conducted no assessment of ML/TF vulnerabilities of specific types of legal persons and arrangements.

18. Assessment of ML/TF vulnerabilities in the VASP sector was conducted by the CFSSA in coordination with the AMLO on the basis of a self–developed methodology. Outcomes were

[19] Vulnerabilities of business activities related to virtual currencies. May 2021, p.2
[20] Idem, p.3
[21] Idem, p.4–5
[22] The World Bank team's role was limited to: (1) Delivery of the tool; (2) Providing guidance on the technical aspects of the tool; (3) Review of draft NRA documents and providing feedback to assist in the accurate use of the tool.

adopted in May 2021 by the President of the CFSSA Management Board. This assessment of a new type of RE designated starting from 2020 was conducted based on information gathered through meetings with the VASP sector, financial analysis, including analysis of transaction (number and volume) and the client base, outcomes of the off–site inspection, filed STRs and regulatory framework.

19. In deciding what issues to prioritise, the assessment team reviewed information and documents provided by Croatia on national ML/TF risks, and information from reliable third–party sources (e.g., reports by other international organisations). Not only do the issues listed present the areas of higher ML/TF risks (including threats and vulnerabilities), but also issues that were of significant concern to the assessment team based on material provided before the on–site visit.

20. **The use of cash** – The shadow economy accounts for a significant part of the GDP of Croatia (more than 30% in 2016 according to the IMF[23] (6,97% in the same year according to the EUROSTAT). The share of cash in total payment transactions in Croatia in 2019 is estimated at 73%[24]. Significant amounts of cash are used in the tax crime schemes (e.g., VAT carousel)[25], in corruption, in purchasing real estate, including in criminal schemes (e.g., purchase and sale of real estate below the market price). In addition, certain REs (e.g., exchange offices) tend to structure larger cash transactions into several smaller ones below the identification threshold[26]. The assessors have focused on (i) the understanding of the ML risks posed by the widespread use of cash and the adequacy of measures to mitigate those, in particular in the banking sector, by MVTSs, exchange offices, casinos, and the real estate sector; (ii) effectiveness of enforcement of introduced cash restriction measures in curbing ML through the use of cash; (iii) the measures taken to prevent, detect and pursue tax–related ML; and (iv) effectiveness of border controls to detect false/non–declarations and identify ML/FT suspicions.

21. **Drug trafficking:** Croatia is one of the countries along the so–called "Balkan route", which continues to be the largest heroin trafficking corridor[27]. It is primarily a transit country along the Balkan route for maritime shipments of South American cocaine bound for Western Europe and other illicit drugs and chemical precursors to and from Western Europe[28,29]. Domestic production of drugs is limited and primarily aimed at satisfying domestic needs, but separate cases of international drug market supplies have been identified[30]. The assessment team have focused on (i) effectiveness of measures in place to combat drug trafficking and discuss the challenges that LEAs may face in this respect, (ii) the extent to which ML related to drug trafficking is prioritised by law enforcement agencies (LEAs), co–operation with customs is effective, and whether the capacities and resources of LEAs are sufficiently adequate; (iii) adequacy of preventative measures implemented by the REs to tackle funds related to drug trafficking.

---

[23] IMF Working Paper WP/19/278 "Explaining the Shadow Economy in Europe: Size, Causes and Policy Options", p.7. There is no open–source information available for more recent years.
[24] https://www.statista.com/statistics/1094775/cash–use–in–croatia/
[25] NRA, p.9
[26] NRA, p.162 "On 1st January 2018 Croatia introduced new CDD rules for exchange offices: the threshold for conducting CDD was lowered from 105 000 HRK (14 000) to 15 000 HRK (2 000 EUR).
[27] https://wdr.unodc.org/wdr2020/en/drug–supply.html
[28] https://www.cia.gov/library/publications/the–world–factbook/geos/hr.html
[29] NRA p.11
[30] NRA, p.11

22. **Corruption:** Criminal offences of domestic corruption and bribery perpetrated by public officials, including cases involving high–ranking officials[31,32,33], constitute one of the most predominant proceeds generating crimes in Croatia[34]. Corruption is commonly conducted through the use of cash, fictitious loans, fictitious companies, real estate, etc. Common elements of domestic corruption include involvement of criminal associations and are characterised by also having an international dimension[35]. The assessors have focused on whether the risks associated with corruption as a source of proceeds of crime have been adequately assessed and whether mitigating measures are adequate and effective (including PEP–related CDD). The assessors have also focused on the potential impact of corruption on the competent authorities' capacity to prevent and pursue ML and economic crime effectively. This included focusing on the operational independence and effectiveness of the competent authorities, including the FIU, LEAs, and the judicial system.

23. **Organised crime:** In Croatia, major proceeds generating crimes (posing high and medium level threats) are largely committed in the context of criminal association, including by the organised criminal groups (OCGs), often with international dimension[36] to both the predicate crime and the ML[37]. Only in 2018, Croatia indicted ten criminal associations involved in drug trafficking. The assessment team have focused on the extent to which ML related to OCGs is prioritised by LEAs and whether the LEAs have adequate capacity to detect and pursue OCG–related ML (especially 3rd party, foreign predicate–related and stand–alone ML) and the manner in which these cases are investigated and prosecuted.

24. **Investigation and prosecution of ML:** The number of ML investigations and prosecutions are considerably lower compared to the predicate criminality for the major proceeds generating offences[38]. The NRA identifies issues related to qualifying an offence as ML due to restrictive interpretation of essential elements of the ML offence provided by the Supreme Court judgements[39]. Despite legal entities being involved in ML and predicate offences frequently, a very low number are being prosecuted. There are certain delays in criminal proceedings for ML and other complex predicate offences, which may impact the effectiveness of the judicial system. The assessment team have focused on (i) determining the investigative priorities of the LEAs and level of attention to ML investigations and prosecutions; (ii) the impact of the legal opinion of the Supreme Court on ML investigations and prosecutions; (iii) the reasons for the possible lack of application of existing sanctions for legal persons under criminal law; and (iv) the reasons for lengthy criminal court proceedings and their consequences.

---

[31] https://www.euractiv.com/section/justice–home–affairs/news/croatias–secret–club–scandal–exposes–cronyism–corruption/
[32] https://www.total–croatia–news.com/politics/28143–todoric–croatia–is–managed–by–plenkovic–s–secret–society–not–the–government
[33] http://www.rai–see.org/croatia–zdravko–mamic–former–head–of–croatian–club–dinamo–zagreb–faces–corruption–charges/
[34] NRA, p.12
[35] https://www.occrp.org/en/component/tags/tag/croatia
[36] https://www.europol.europa.eu/newsroom/news/croatian–police–arrest–and–dismantle–organised–crime–group–in–large–international–investigation
[37] NRA, p.5
[38] MEQ on Effectiveness, page
[39] NRA, p.4

25. **Mutual legal assistance (MLA) and international co–operation**: ML and a considerable number of major proceeds generating predicate offences (e.g., OCGs[40], drug[41,42] and human[43] trafficking) have a significant cross–border element in Croatia. The existence of robust MLA mechanisms and other forms of international co–operation is therefore essential for Croatia. The assessment team have focused on the manner in which Croatian authorities provide MLA and co–operate with their foreign counterparts through other means and whether they proactively seek international assistance. Due to the significant presence of foreign banks within Croatia, the assessment team have also examined the effectiveness of co–operation between the domestic and foreign supervisory authorities.

26. **TF risk understanding:** The Western Balkans are targeted by Al–Qaeda, the so–called Islamic State, and affiliated groups for expanding the number of followers[44]. Nevertheless, the external sources confirm Croatia is not a major source country for foreign fighters travelling to the conflict areas of the Middle East[45]. There has been no TF investigation in Croatia, and only two foreign requests were received over the past period. The assessors have examined these international co–operation requests and applied measures. In addition, the assessment team have further analysed understanding of TF risks, the possible impact of OCG and migrant smuggling on TF risks, abilities and adequacy of resources of the LEAs for detecting, investigating and prosecuting TF. Special attention was paid to the TF risks related to the NPO sector abuse, which was an area of limited focus in the NRA, examining (i) understanding of TF risks by the supervisory authorities and the private sector, (ii) adequacy of applied preventative measures, and (iii) implementation of the TF–related UNSCRs.

27. **Virtual Assets:** Croatia has recently introduced a regulatory framework for certain types of virtual asset services and a notification mechanism for keeping the list of registered VASPs. There are gaps in the regulatory framework of Croatia, no licensing and monitoring mechanism for AML/CFT purposes has been implemented. The authorities conducted the VASP vulnerability analysis, presenting some high–level findings on the market size and structure. The team focused on the understanding by the country of risks associated with the VASPs use of VAs and the measures taken to mitigate them**.**

28. **Financial institutions:** Banking and the MVTS sectors are identified as most featured in criminal investigations. The NRA highlights that organised crime and corruption are conducted using sophisticated methods of concealment of money, such as internet banking[46]. ML is also committed by using "money–mule" bank accounts[47], as a part of an international OCG. The MVTS sector has been misused in computer fraud schemes[48]. The assessment team have examined the understanding of ML/TF risks by these sectors and the application of preventative measures by

---

[40] https://www.soa.hr/en/areas–of–activity/organized–crime/#:~:text=Croatia's%20transport%20connections%20and%20geopolitical,routes%20between%20Europe%20and%20Asia.&text=Organized%20crime%20has%20developed%20irrespective%20of%20national%20borders
[41] https://www.emcdda.europa.eu/countries/drug–reports/2019/croatia/drug–markets_el
[42] https://wdr.unodc.org/wdr2020/en/drug–supply.html
[43] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680630e7c
[44] https://www.europol.europa.eu/newsroom/news/targeted–propaganda–material–disseminated–in–languages–of–western–balkan–countries
[45] https://www.osac.gov/Country/Croatia/Content/Detail/Report/e4f2e6e9–d9e2–4b7b–8505–15f4aead7e72#:~:text=There%20is%20minimal%20risk%20from,areas%20in%20the%20Middle%20East.
[46] Annual Report on the work of state attorney's offices, 2018
[47] https://www.riskscreen.com/kyc360/news/gardai–move–against–fraudsters–engaged–in–covid–19–scam/
[48] NRA, p.19

these and other financial institutions. Special attention has been paid to the implementation of CDD measures and the ability to identify the BO and report STRs.

29. **DNFBPs:** Lawyers, public notaries, accountants and real estate agents among the DNFBP sector are frequently used in ML schemes[49]. Among services provided by the lawyers, public notaries, and accountants, the following are considered to be of higher exposure to ML: (i) services of opening and conducting financial transactions on behalf of and for the account of clients; and (ii) establishment, operation or management of trusts, companies, foundations or similar legal arrangements. All these REs are also involved in transactions related to real estate acquisition, which is assessed as a high–risk product. The real estate brokerage sector is specified as risky in combination with other sectors (lawyers, notaries public and credit institutions)[50,51]. The STR statistics provided by the authorities appear to demonstrate that these sectors file limited numbers of STRs. The assessment team have focused on understanding the ML/TF risks and the implementation of preventative measures, including identification of BO by the mentioned DNFBPs, risks related to provision of trust services, and knowledge of ML typologies in use of the provided services.

30. **Transparency of legal entities and beneficial ownership**: Legal persons are often misused for laundering proceeds of crime in Croatia, especially proceeds of tax evasion and fraud. The use of frontmen to conceal the real ownership of assets held by Croatian companies, the setting up of complex corporate structures involving foreign entities, as well as the use of fictitious companies have been detected as ways to launder and conceal the proceeds of crime. The assessment team have focused on the effectiveness of mechanisms put in place to ensure the transparency of legal persons and the availability of accurate BO information of companies. Attention has been given to challenges arising from the: (i) the ability to open Croatian companies online with or without intervention of legal professions, (ii) the faculty of creating secretive silent, partnerships that may be abused to obscure ownership of companies.

### 1.2. Materiality

31. Croatia is one of the smaller economy EU Member States[52], with a GDP of approximately EUR 53.97 bn in 2019[53] and an average annual growth rate of 2.4%54 in 2014–2019. The Croatian economy is highly open and service–oriented. The most important sectors of Croatia's economy in 2019 were manufacturing (12%), wholesale/retail trade (10.2%), real estate sector (7.3%), accommodation and food service (5.4%), financial and insurance sector (4.8%)[55] and construction 4.6%). Intra–EU trade accounts for 68% of Croatia's exports. Outside the EU, the major export destinations are Bosnia & Herzegovina (9%) and Serbia (4%). In 2019, the most exported goods were related to food products, pharmaceutical products, electrical equipment, machinery and equipment[56]. In terms of imports, 78% come from EU Member States, while outside the EU, the major importing states are Bosnia & Herzegovina and China (3% come from

[49] NRA, p. 205, 208, 211 and 217
[50] NRA, p.217
[51] https://www.riskscreen.com/kyc360/news/unreal–estate/
[52] Croatia has entered the European Union in 2013 and became the latest entrant to the EU. It is not a signatory of Schengen Agreement.
[53] https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=HR&name_desc=false
[54] https://www.hnb.hr/en/statistics/main–macroeconomic–indicators
[55] This number comprises entire insurance sector including life insirane
[56] https://www.dzs.hr/Hrv_Eng/publication/2019/04–02–01_12_2019.htm

both)[57]. In 2019, most imported goods were related to food products, chemicals, motor vehicles, machinery and equipment, computer and electronic products[58].

32. In 2019, the foreign direct investment flows to Croatia amounted to EUR 1.3 bn. The top 3 investment countries were Luxembourg (22%), Austria (19.7%), and Slovenia (10.8%). The economic sectors most attractive to investors included financial services (22%), manufacturing (18%), trade (16%), real estate and construction (10%), telecommunication (6%) and tourism (5%)[59].

33. Croatia is not an international financial centre. The financial sector in Croatia is dominated by the banking system accounting for more than 66% of total financial sector assets at the end of 2019. Pension funds and insurance companies come next, with a share of 18% and 7%, respectively. In 2019 the ratio of banking sector assets to GDP was 108.5%, while that of the whole financial sector was 162%. The two biggest banks hold 48% of the banking industry's total assets, and the five biggest banks hold 81%[60]. A large majority of the banking system (90.5%) is foreign owned[61]. Four credit institutions in Italian ownership accounted for nearly half of total credit institutions' assets (49%). Six credit institutions in Austrian and one in Hungarian ownership followed, with a share of 30% and 10%, respectively. Three banks, which accounted for 1% of total credit institutions' assets, were majority–owned by shareholders from the Czech Republic, San Marino and Turkey. At the end of 2019, three banks had four foreign subsidiaries – two in Bosnia and Herzegovina, one in Slovenia and one in Montenegro.

34. Most of the bank accounts are owned (and the highest volume of transactions are conducted) by the residents of Croatia (96,9% of the funds held by January 2020). The figures for non–residents are minor in nature (3,1% of the funds held by January 2020).

35. In Croatia, the majority of the total turnover in the provision of money remittance services (96%) is carried out through the non–banking sector. The total volume of transactions conducted by MVTSs in 2020 amounted to approximately EUR166 mln.

36. The AMLTFL provides for a limited exemption in relation to electronic money. This has been directly transposed from the 4th AML Directive and not supported by the risk assessment. Two types of REs are not properly designated, and hence the FATF Recommendations do not apply to: (i) external accountants and (ii) VASPs, except for those engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. Nevertheless, these sectors are not significantly material in Croatia.

37. Among the DNFBPs, the real estate sector is one of the attractive sectors for foreign investments (mostly from Slovenia, Germany, and Austria) and is estimated at EUR 5.15 bn[62] in 2019 (9.54% to GDP). In 2019, the ratio of the casino sector to GDP was about 1,09% (EUR 557 mln.). Among these, land–based casinos accounted for around 27,33% of the total sector, and online casinos – 72,67%. There are no ship–based casinos in Croatia.

38. Croatia is not a signatory to the Hague Convention on Laws Applicable to Trusts and Their Recognition. Therefore, there is no statutory basis for the establishment of legal arrangements,

---

[57] https://europa.eu/european–union/about–eu/countries/member–countries/croatia_en
[58] https://www.dzs.hr/Hrv_Eng/publication/2019/04–02–01_12_2019.htm
[59] http://investcroatia.gov.hr/en/about–croatia/
[60] First five banks by the asset size are Zagrebačka banka d.d., Privredna banka Zagreb d.d., Erste&Steiermärkische Bank d.d., OTP banka d.d. and Raiffeisenbank Austria d.d.
[61] Data provided by Croatian authorities in Effectiveness Questionnaire
[62] Tax administration data on the value of real estate purchase contracts that have been reported for taxation

but the AML/CFT legislation recognises trust and company service providers as designated entities. Nevertheless, Croatia detected one company[63], the activity of which includes among others the provision of fiduciary, office rentals, virtual offices and business address rentals services. In addition, trust and company services for the establishment and management of companies and other legal arrangements in Croatia are provided by law firms, independent lawyers and external accountants. Notaries public provide assistance for establishment, operation or management of trusts, companies, foundations or similar legal arrangements[64]. While there is no estimation of the size of the business itself, the total revenue of the above indicated legal professions is estimated to amount approximately to EUR 752 (1,75% to GDP)[65].

### 1.3. Structural Elements

39. The key structural elements for effective AML/CFT control are generally present in Croatia, including political and institutional stability, accountability, transparency, and the rule of law. There is a high–level political commitment to address AML/CFT issues, which, in the view of the assessment team, needs to be further strengthened (see Immediate Outcome 1). AML/CFT coordination is conducted through the IIWG. The IIWG is an expert working group[66] composed of representatives of 11 institutions involved in the prevention of ML/TF. This does not include policymakers[67] – any senior officials, except for the representatives of the SAO.

40. The level of perceived judicial independence remains among the lowest in the EU. This is due to numerous factors, including insufficient staffing, material and technical resourcing, efficiency and quality challenges, political influence in selecting and appointing judges and state attorneys[68]. Furthermore, there are weaknesses in the judicial system, particularly in terms of restricted understanding of ML, driven by the Supreme Court interpretation of ML offence[69], and undue delays in the criminal court proceedings. International reports point out integrity issues in the judiciary and the police[70].

### 1.4. Background and Other Contextual Factors

41. Croatia has an increasingly mature AML/CFT system, albeit there is room for improvement in sensitive areas. Since the last evaluation of the country in 2013, Croatia has initiated important changes in its AML/CFT Law on two occasions, transposing into domestic framework Directive (EU) 2015/849 (the so–called 4th AML Directive) in 2017 and Directive (EU) 2018/843 (the so–called 5th AML Directive) in 2019. This allowed Croatia to follow global AML/CFT framework developments, expanding the domestic AML/CFT preventative system.

---

[63] https://www.tmf–group.com/en/locations/emea/croatia/
[64] NRA, p.208, 223
[65] Calculated on the basis of figured provided in the NRA, p.205, 207 and 211
[66] AML/CFT Law, Art.4(23)
[67] AMLO – Deputy Director, 3 Heads of Services; Financial Inspectorate – 3 Heads of Services; Tax Administration – 2 Tax advisors, Head of Service, Senior Specialist Advisor; Customs Administration – Senior Inspector; Ministry of Interior – 2 police officials; Ministry of Justice and Administration – Head of Service; Ministry of Foreign and European Affairs – Head of Service; State Attorney's Office – First Deputy Attorney General, Deputy Attorney General, Deputy Municipal State Attorney; Croatian National Bank – Director of Department, Chief Advisor; Croatian Financial Services Supervisory Agency – Head of AML Office, Senior Supervisor; Security Intelligence Agency – operative officials.
[68] EU Commission, 2020 Rule of Law Report, p.1
[69] The Supreme Court of the Republic of Croatia, I Kž 625/13–6 of 28 May 2015, and I Kž 560/16–4 of 28 November 2016
[70] EU Commission, 2020 Rule of Law Report, and GRECO, 2019 Fifth Round Evaluation Report on Croatia.

42. Financial exclusion is not a widespread issue in the country, as according to the G20 Financial Inclusion Indicators in 2017, about 86% of inhabitants dispose of a bank account, whereas 83% above the age of 15 engage in digital payments[71].

43. The GRECO evaluation report on Croatia (fifth evaluation round – Preventing corruption and promoting integrity in central governments (top executive functions) and law enforcement agencies) adopted in December 2019 states that "Corruption is widely perceived as a major issue affecting Croatia." In Transparency International's 2020 Corruption Perceptions Index, Croatia scores 47 (out of a total score of 100), placing it at 63 out of the 180 countries included in the survey. Croatia has implemented the Anti–Corruption Strategy 2015–2020, which focused primarily on the prevention of corruption. The Anti–Corruption Strategy for the period from 2015 to 2020 was implemented through three two–year Action Plans (2015–2016, 2017–2018 and 2019–2020). According to official data, Action Plans were implemented for over 80%. Improvements were made in the legislative and institutional frameworks. In particular, these concerned whistle–blowers protection, managing conflicts of interest, raising public sector transparency, public procurement, public property management etc. A new Strategy on the Prevention of Corruption for 2021–2030 is in the public consultation process. The primary focus areas of the strategy will be on prevention, strengthening the institutional and legal framework for fighting corruption, raising awareness on the harmfulness of corruption in the general public, increasing transparency of the work of public bodies and improving integrity systems in numerous priority areas[72].

### *1.4.1. AML/CFT strategy*

44. Croatia does not have a formal AML/CFT Strategy in place. The 2015 National Strategy for the Prevention and Suppression of Terrorism was adopted and serves as a key strategic document in the area of counterterrorism and contains some actions concerning TF. Based on the two NRAs (from 2016 and 2020), Croatia developed the respective Action Plans that include measures aimed at mitigating the identified ML/TF risks. The latest Action Plan consists of 13 actions cumulatively focused on (i) enhancing the capacities of the AML/CFT authorities by conducting training and education, strengthening administrative capacities, enhancing co–operation and communication; (ii) increasing AML/CFT supervision (by CFSSA); (iii) providing regular feedback to REs (by AMLO); (iv) collecting information form DNFBPs for risk assessment purposes (Financial Inspectorate and TA).

### *1.4.2. Legal & institutional framework*

45. The Anti–Money Laundering and Terrorist Financing Law (AMLTFL) is the central piece of legislation on AML/CFT matters. It requires the application of preventive measures, including STR reporting, by REs (including virtual currency exchange service providers since 2020), the conduct of AML/CFT supervision by relevant authorities, and establishes sanctions. It also provides for the establishment and functioning of the AMLO and the IIWG. Other relevant pieces of legislation include the sectorial laws regulating the financial and DNFBP sector, the Criminal Code (CC), the Criminal Procedure Code (CPC), Law on International Restrictive Measures, and other sectorial legislation.

46. The institutional framework involves a broad range of authorities. The most relevant are the following:

---

[71] https://datatopics.worldbank.org/g20fidata/country/croatia
[72] Draft proposal of the Anti–Corruption Strategy 2021–2030 p.5.

47. **The Inter–institutional Working Group on Money Laundering and Terrorist Financing (IIWG)** is an expert working group[73] composed of representatives from eleven institutions involved in the prevention of ML/TF. Performance of the IIWG tasks is directed and coordinated by the AMLO (FIU)[74]. The IIWG coordinates national ML/TF risk assessment. The IIWG is tasked to conduct a risk assessment, develop an action plan for implementation of respective measures, implement the NRA and carry other analytical tasks. There are two sub–working groups that operate within the IIWG: (a) the Supervisory Subgroup – for co–operation and coordination among the supervisory and monitoring authorities and (b) the Operational Subgroup – for coordination of actions and mutual feedback on specific ML/TF cases among the authorities vested with intelligence gathering and law enforcement functions.

48. **The Anti–Money Laundering Office (AMLO)** is the Croatian FIU that operates within the Ministry of Finance (MoF) as an organisational unit that independently performs its tasks. It is in charge of the receipt and analysis of STRs, threshold transaction reports, cross–border cash reports[75], and other information communicated by public or private agencies or individuals, and dissemination to LEAs and other competent authorities and foreign counterparts.

49. **Ministry of Justice and Administration (MoJA)** is the central authority for the receipt of MLA and extradition requests. The MOJA is responsible for the state regulation and supervision of the court and SAO and over the work of the notary public service. It oversees the drafting and implementation of laws and other regulations in the field of criminal law. The MoJA coordinates the development and implementation of national strategies and implementation documents in the field of anti–corruption.

50. **State Attorney's Office (SAO)** supervises the Police's actions in conducting preliminary investigations and leads criminal investigations of all criminal offences. The Office for the Suppression of Corruption and Organised Crime (USKOK) is a specialised department within the SAO with the competencies to investigate ML; Criminal Association; Corruption and bribery; Tax or Customs Duty Evasion, and other offences. TF and other terrorism–related offences are dealt with by the County SAO. ML, other than that falling under the competence of the USKOK is dealt with by the Municipal State Attorneys. Country SAO have respective competencies for the receipt and execution of European Investigation Orders (EIOs) and European Arrest Warrants (EAWs).

51. **Ministry of Interior (MoI)** handles tasks related to police, criminal police, border police and special police activities. Within the MoI, a Police Directorate has been set up. Within the Police Directorate, the Criminal Police Directorate has been established with its constituents Police National Office for Suppression of Corruption and Organised Crime (PNUSKOK), the General Crime and International Police Co–operation Sector and the Criminal Intelligence Sector. The Economic Crime and Corruption Service within the PNUSKOK is the national contact point (Asset Recovery Office–ARO) for the submission of requests and exchange of data for the purpose of tracing and identifying proceeds of crime.

52. **Customs Administration (CA)** is the administrative structure within the MoF with core responsibilities for the application of customs, excise, tax and other regulations. It controls the application of cash declaration requirements at national borders. The CA files the cross–border cash transactions reports to AMLO.

---

[73] AML/CFT Law, Art.4(23)
[74] AML/CFT Law, Art.5(5)
[75] The reference to cash includes bearer–negotiable instruments and currency.

53. While the CA is not vested with law enforcement powers, the SAO can appoint an authorised official from custom administration as an investigator to perform evidentiary actions entrusted to him by the competent State Attorney in accordance with the provisions of the CPC and regulations within the respective administration.

54. **Ministry of Foreign and European Affairs (MFEA)** is responsible for the legislation on international sanctions, including targeted financial sanctions on TF and PF.

55. **Croatian National Bank (CNB)** is responsible for issuing and revocation of authorisations, licences and approvals for financial institutions, and conducting AML/CFT supervision over banks, housing saving banks, credit unions, electronic money institutions and payment institutions.

56. **Financial Inspectorate (AML/CFT Supervision Unit)** is an administrative structure within the MoF responsible for AML/CFT supervision of financial market participants, such as authorised exchange offices, MVTSs (agents by payment service providers from another Member State, Croatian Bank for Reconstruction and Development (HBOR) and consumer credit service providers) and DNFBPs, such as lawyers, notaries public, accountants and tax advisors, auditors, real estate brokers, dealers in precious metals and stones, dealers in art objects and antiquities, auctions, TCSPs. Financial Inspectorate is not vested with licensing or authorisation powers.

57. The Financial Inspectorate (Misdemeanours Court) conducts first instance misdemeanour proceedings for violations of the provisions of the AMLFTL and the acts regulating prevention of ML/TF, foreign currency operations and the providing of payment operation and money transfer services.

58. **Croatian Financial Services Supervisory Agency (CFSSA)** is responsible for issuing and revocation of authorisations, licences and approvals. It also exercises supervision of AML/CFT measures over investment firms, life insurance companies, life insurance intermediaries, investment funds management companies, investment funds with legal capacity, pension companies managing voluntary pension funds, pension insurance companies, leasing companies, and factoring companies. The CFSSA is also responsible for the registration of legal and natural persons engaged in the activities of provision of exchange services between virtual currencies and fiat currencies and provision of custodian wallet services (VASPs), and conducting AML/CFT supervision.

59. **Tax Administration (TA)** is an administrative structure within the MoF with core responsibilities for implementing tax and other compulsory payments regulations. It is also responsible for licensing and supervision, including on AML/CFT matters of organisers of games of chance (lottery games, casino games, betting games, slot–machine gaming, games of chance via Internet, telephone or other interactive communication means (on–line gaming)). TA exercises supervision over the BO Register.

60. While TA is not a law enforcement authority, it includes an independent Sector for Financial Investigations responsible for pursuing financial investigations of predicate offence. In addition, when necessary, the SAO can appoint an authorised official from TA as an investigator to perform evidentiary actions pursuant to CPC.

### *1.4.3. Financial sector, DNFBPs and VASPs*

61. An overview of the financial and non–financial sector is provided in the table below.

**Table 1.1: Number and size of financial institutions operating in Croatia**

| Reporting Entity | Number of licensed/registered entities | Size of the sector Assets /Total assets (December 2020) |
|---|---|---|
| Banks[76]:<br>– operating<br>– under bankruptcy proceedings<br>– under winding–up proceedings | <br>20<br>8<br>5 | EUR 61 000 000 000 – assets |
| Branches of foreign banks<br>– operating | <br>1 | EUR 400 000 000 – assets |
| Housing savings banks[77]:<br>– operating<br>– under winding–up proceedings<br>– authorisation was revoked, but have not initiated winding–up proceedings | <br>3<br>1<br>1 | EUR 693 000 000 – assets |
| Credit unions[78]:<br>– operating<br>– under bankruptcy proceedings<br>– under winding–up proceedings | <br>17<br>3<br>11 | EUR 82 000 000 – assets |
| Payment institutions[79]<br>– operating | <br>3 | EUR 3 000 000 – asset<br>EUR 40 950 – volume of transactions [80] |
| Electronic money institutions[81]<br>– operating | <br>5 | EUR 2 221 000 000 – asset<br>EUR 2 941 033 268 – volume of transactions [82] |
| Life insurance companies<br>– operating | <br>11 | EUR 3 355 000 000 – asset<br>EUR 353 000 000 – gross written premium |
| Subsidiaries of foreign life insurance companies<br>– operating | <br>1 | EUR 6 000 000 – gross written premium |
| Investment funds management companies<br>– operating | <br>23 | EUR 3 053 000 000 – net asset value |
| Investment funds (having a legal status and internal management)<br>– operating | <br>2 | EUR 17 000 000 – net asset value |

[76] https://www.hnb.hr/en/core–functions/supervision/list–of–credit–institutions
[77] Idem
[78] https://www.hnb.hr/en/core–functions/supervision/list–of–credit–unions
[79]https://www.hnb.hr/en/core–functions/payment–system/registers–and–records/register–of–payment–service–providers–and–electronic–money–issuers
[80] The transaction amount of Payment institutions in 2020 includes the acceptance of national and international payment transactions by credit cards issued by credit institutions and EMIs in Croatia.
[81] Idem
[82] The transaction amount of Electronic money institutions in 2020 includes electronic money purchases – prepaid/SMS/prepaid SIM, national and international payment transactions by credit cards issued by EMI in the RC, the acceptance of international payment transactions by credit cards issued outside the RC by EMI and the service of bill–paying via self–service devices.

| | | |
|---|---|---|
| Pension companies managing voluntary pension funds<br>– operating | 4 | EUR 829 400 000 –net asset value |
| Pension insurance companies<br>– operating | 2 | EUR 192 000 000 – assets<br>EUR 97 000 000 – revenues |
| Investment firms<br>– operating | 6 | EUR 6 000 000 – revenue |
| Leasing companies:<br>– operating<br>– under winding–up proceedings | 15<br>6 | EUR 2 627 000 000 – asset<br>EUR 100 000 000 – asset |
| Factoring companies<br>– operating<br><br><br>– under winding–up proceedings | 4<br><br><br>1 | EUR 43 000 000 – asset<br>EUR 132 000 000 – volume of transactions<br>EUR 160 000 – asset<br>EUR 1 000 000 – volume of transactions |
| Authorised exchange offices[83]<br>– operating | 1188 | EUR 1 847 000 000 – purchase<br>EUR 718 000 000 – sale |
| MVTSs<br>– operating Money remittances<br>– Croatian Post | 3(52) | EUR 106 000 000 – volume of transactions for money remittances<br>EUR 60 000 000 – volume of transactions for postal orders |
| Croatian Banks of Reconstruction and Development | 1 | EUR 3 805 000 000 – asset |
| Consumer credit service providers | 1 | EUR 2 000 000 – asset |
| Legal and natural persons providing exchange services between virtual currencies and fiat currencies and custodian wallet services (VASPs)*<br>– Registered with the CFSSA | 15 | EUR 62 037 799– volume of transactions |

**Table 1.2: Number and size of DNFBPs operating in Croatia**

| DNFBP Sector | Number of licensed/registered entities | Size of the sector total revenue/turnover (2020) |
|---|---|---|
| Lawyers | 3669[84] | EUR 336 000 000 – revenue |
| Notaries public | 312 | |
| Accountants | 5227[85] | EUR 426 000 000 – revenue |
| Tax advisors | 43 | |
| Auditors | 206 | |
| Real estate brokers | 1 198 | EUR 85 000 000 – revenue |

[83] https://www.hnb.hr/en/core–functions/payment–system/authorised–exchange–offices
[84] Out of registered 3569 persons, 1183 declared themselves subject to the AMLTFL.
[85] Tax Administration data on entities that have reported revenues registered under *NKD* (National Classification of Activities) 69.20

| | | |
|---|---|---|
| Lottery | 1 | EUR 102 000 000 – turnover |
| Casino | 19 | EUR 18 000 000 – revenue |
| Betting | 7 | EUR 204 000 000 – turnover |
| Gambling on slot machines | 45 | EUR 161 000 000 – revenue |
| Online gambling | 8 | EUR 106 000 000 – revenue (online casino)<br>EUR 388 000 000 – turnover (online betting) |
| Dealers in precious metals and stones | 108[86] | EUR 77 000 000 – turnover |
| Dealers in art objects and antiquities, auctions | 38[87] | EUR 600 000 – turnover |
| Trusts and company service providers | 1[88] | EUR 1 628 000 000 – revenue |

62. The assessors ranked the financial and DNFBP sectors based on their relative importance in Croatia, given their respective materiality and level of ML/TF risks. Throughout this report, the assessors used these rankings to inform their conclusions, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report but is most evident in IO.3 and IO.4.

63. **The banking and MVTS sectors are weighted as being the most important in Croatia's context based on their materiality and risks.** In 2019 the ratio of banking sector assets to GDP was 108.5%, while that of the whole financial sector was 162%. The two biggest banks hold 48%[89] of the banking industry's assets, and the five biggest banks hold 81%[90]. The majority of banks are members of a banking group. While the NRA assessed the banking sector as being at a medium–high risk for ML/TF both in 2016 and in 2020, it acknowledges the high attractiveness of the banking sector for misuse by criminals, including through the use of legal persons. The NRA highlights, in particular, that "the Banking Sector is somewhat more exposed to ML risk than some other sectors. A significant number of ML activities begin or at some stage go through the Banking Sector"[91]. When weighting the sector, the assessment team has also taken into consideration the supervisory findings in one of the largest banks operating in Croatia.

64. In Croatia, the majority of the total turnover in the provision of **money remittance services** (96%) is carried out through the non–banking sector. The total volume of transactions conducted by MVTSs[92] in 2020 amounted to approximately EUR166 mln.. The conducted transactions in the sector are predominantly of a cross–border nature. The sector is characterised as cash–intensive. Both factors increase the exposure of the sector to ML/TF risks.

65. **Authorised exchange offices, casinos and gambling operators and VASPs are weighted as being important in Croatia's context based on their materiality and risks**.

66. The total turnover of the **authorised exchange sector** in 2020 amounts to about EUR 2 565 mln. (including purchase and sale). The sector is considered significant, with high exposure to

[86] Number of entities subject to the AMLTFL and turnover are the estimation of the Croatian authorities.
[87] Idem
[88] Idem
[89] Zagrebačka banka d.d. and Privredna banka Zagreb d.d.
[90] First five banks by the asset size are Zagrebačka banka d.d., Privredna banka Zagreb d.d., Erste&Steiermärkische Bank d.d., OTP banka d.d. and Raiffeisenbank Austria d.d.
[91] NRA 2020, p.58
[92] This includes also figures for the Croatia Post.

cash. The sector is exposed to structuring of operations through conducting below customer identification threshold transactions. The Supervisory findings also point out issues related to poor performance of CDD requirements. The NRA assessed the authorised exchange sector as being at medium risk for ML/TF. Taking into account the size of the sector, use of cash and vulnerabilities present in the sector, the assessment team considered the sector to be important.

67. The total annual revenue of the **gambling sector** in 2019 amounted to about EUR557 mln.[93][94]. Land–based casinos are often associated with hotels, more specifically in the coastal areas. Hotels have the highest number of land–based casinos to complement the hotel business. In addition, the gambling sector, except for on–line gambling, is characterised by high exposure to cash[95]. These two factors are increasing the sector's ML/TF risks. Online gambling is a segment with a growing interest in the population. Customers are offered games via the internet, telephone, and other interactive communication devices. In 2020 the revenue of online casinos was estimated at the level of EUR 106 mln. Based on these factors the assessment team considered the gambling sector to be important.

68. The authority's estimation of the annual volume of transactions conducted by **VASPs** in 2020 amounts to EUR 62 mln.[96]. Croatia applies the pre–existing AML/CFT Law to VASPs, applying similar requirements as to FIs. Reporting obligations extended to VASPs starting from 2020. The regulated activities of VASPs covered in Croatia are limited to the ones provided in the EU 5th AML Directive. The vulnerabilities assessment conducted by the Croatian authorities ranks them as being at moderate level for ML/TF, mostly for the gaps in the regulatory framework. At the time of the on–site, there were 15 VASPs identified operating in the market, one of which co–operated with Croatia Post using the net of the post offices around the country for providing crypto–exchange services[97]. Open–source information suggests the market is being populated with more participants who have not yet notified the CFSSA. These factors cumulatively formed the basis for the assessment team to consider this sector as important.

69. **Housing savings banks, leasing companies, electronic money institutions, lawyers, accountants, tax advisors, notaries public, real estate brokers and dealers in precious metals and stones are weighted as being moderately important in Croatia's context based on their materiality and risks.**

70. The total assets of the **housing savings banks** in 2020 amounted to about EUR 693mln. There are three housing savings banks operating in the country, of which two are members of a banking group, and the other is a member of a European financial group providing housing saving loan services. These are financial institutions with a customer base consisting of natural persons (Croatian citizens), obtaining loans for purchasing real estate. Although Croatia recognises real estate as a high–risk product, considering the legally limited scope of the activities that are aimed at providing loans with the financial support of the state, while bearing in mind the ML risks

[93] https://www.fina.hr/novosti/–/asset_publisher/pXc9EGB2gb7C/content/poduzetnici–u–djelatnosti–kockanja–i–kladjenja–u–10–godina–udvostrucili–ukupne–prihode?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_pXc9EGB2gb7C_assetEntryId=615393

[94] In line with the available figures for 2020 the total revenue of casino, gambling on slot machines and online gambling together amounted to EUR 567mln., and the total turnover of lottery, betting and the online gambling amounted to EUR412mln.

[95] NRA, p.197 "The Tax Administration estimates that 70% of casino turnover is done in cash (payment and withdrawal)".

[96] Idem, p.3

[97] https://www.wibestbroker.com/crypto–projects–in–croatia/

associated with real estate, the assessment team deems the mentioned factors suggest the sector to be moderately important.

71. The total assets of the **leasing companies** in 2020 amounted to about EUR2 627mln. Croatian authorities concluded this sector to be at a level of Medium risk for ML/TF. There are currently 15 leasing companies operating, and 6 are under winding–up proceedings. The supervisory findings suggest a need to increase the CDD capacities of the sector. Similarly, **electronic money institutions** are considered to be at a level of Medium ML/TF[98] risk. The total volume of transactions conducted in 2020 was EUR2 941mln. The supervisory findings suggest a need to increase detection of existing typologies and STRs.

72. The estimated revenue of **lawyers** (law firms and individual lawyers) was around EUR 53 mln. in 2019. The lawyers provide a wide range of services in Croatia. 37% of the sector does business with higher risk clients: non–residents from the offshore area and from non–EU countries, NPOs, PEPs or customers with a non–transparent ownership structure. Offered services include those caring higher ML/TF risks, such as assistance in purchase and sale of real estate, real estate transactions on behalf of and for the account of clients, conducting financial transactions on behalf of and for the account of clients, establishment, operation or management of trusts, companies, foundations or similar legal arrangements provision of assistance in planning and conducting transactions related to the purchase and sale of business entities[99].

73. The estimated revenue of the **accountants and tax advisors** sectors cumulatively was around EUR 426 ml. in 2020. Most tax advisors also provide accounting services in Croatia. While there is a licensing requirement set for tax advisors, no such requirement exists for accountants, although both are supervised by the Financial Inspectorate. Compared to lawyers, these professions are less engaged with higher risk profile clients. 21% of the profession provides services to non–residents from non–EU countries and 38% – to NPOs. Some representatives of the **accounting and tax advisory** sectors also provide services of renting their business address to clients, opening or managing the client's bank accounts, managing funds, securities or other assets for the customer, conducting real estate transactions for the customers[100].

74. The estimated revenue of the **notary public** was around EUR 16 mln. in 2019. Around 10% of notaries public do business with non–residents from off–shore areas, 67% with non–residents from third countries, and 12% – with NPOs. Notaries public, among others, provide assistance to customers related to establishment, operation or management of trusts, companies, foundations or similar legal arrangements, performing transactions involving real estate on behalf of their client or for their client, purchase or sale of business entities, performing financial transactions on behalf of their client or for their client[101].

75. The estimated revenue of the **real estate brokers** was EUR 85 mln. in 2020. Croatia recognised the purchase and sale of the real estate sector to be a high–risk product. The NRA identified insufficient awareness of ML/TF risks in the sector, especially among brokers that do not conduct financial transactions and consider that they are therefore not obliged to report suspicious transactions. A combination of the high risks present in the real estate market and vulnerabilities in the real estate brokerage sector are considered important factors when deciding on the importance of the sector. Nevertheless, considering the role of brokers in the

[98] NRA 2020, p.169–168 and 174
[99] NRA 2020, p.205–206
[100] NRA 2020, p.206
[101] NRA 2020, p.208–209

Croatian market and materiality of the sector real estate brokers are deemed to be moderately important.

76. The estimated turnover of **dealers in precious metals and stones** was EUR 77 mln. in 2020. The DPMS market is highly concentrated, with the ten largest REs accounting for 90% of the market turnover. Over 80% of the customer base of the DPMS consists of non–resident clients. Some DPMS sell products on–line. The NRA recognises the sector to pose a medium risk. On this basis, the AT considered the sector to be moderately important.

77. **Other FIs and DNFBPs are weighted as being of relatively low importance in Croatia's context based on their materiality and risks.** Among FIs – the life insurance companies, subsidiaries of foreign life insurance companies, investment funds management companies, investment funds (having a legal status and internal management), pension companies managing voluntary pension funds, pension insurance companies, investment firms, factoring companies, consumer credit service providers, and among the DNFBPs – auditors, and trusts and company service providers are considered to be of relatively low importance either on the basis of Croatia's risk assessment or on the basis of the low materiality of the sector.

### *1.4.4. Preventive measures*

78. In Croatia, the preventative measures are set out in the AMLTFL and its associated Rulebooks, accompanied by sectoral guidelines. The previous AMLTFL in place at the time of the previous round of assessment of Croatia was ceased in 2017 with the adoption of the new AMLTFL, which was further revised and amended in 2019. The changes and amendments introduced into the AMLTFL were initially driven by the implementation of the 4th and 5th EU AMLD, meeting recommendations made in the 4th round of MONEYVAL assessment, and advancements of the AML/CFT system in the country.

79. The AMLTFL provides for a limited exemption in relation to electronic money. REs are permitted not to apply certain CDD requirements based on an appropriate risk assessment indicating that the risk is low provided that certain mitigating conditions are met (e.g., limited re–loadability and lack of anonymity). The exemption has been directly transposed from the 5th AML Directive without conducting a risk assessment.

80. There are two types of REs that are not properly designated, and hence the FATF Recommendations do not apply to them. These are external accountants (sector assessed as Medium risk) and VASPs, except for the ones engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. Assessment of vulnerabilities of the VASP sector was conducted recently, concluding that the level of the ML/TF vulnerabilities is Moderate.

81. The AMLTFL is not applicable to financial activities if they are conducted on an occasional and limited basis (e.g., accounting for no more than 5% of the turnover in any accounting period, and with a EUR 1 000 threshold for each individual transaction, etc.) This, for example concerns hotels, gas stations etc., providing exchange services.

82. Croatia extends the application of preventative measures to certain activities that are not covered by the FATF Standards i.e., auditors, tax advisors, dealers in art objects and antiquities, auctions and organisers of games of chance other than casinos.

### *1.4.4. Legal persons and arrangements*

83. Croatia recognises a wide range of legal persons, with LLCs and SLLCs being structures that most often feature in criminal cases, including ML cases.

84. In Croatia, the following types of legal persons may be set up: Companies (which include General Partnerships, LLCs that may take the form of SLLCs, Joint Stock Companies (JSC), Limited Partnerships and Economic Interest Associations), Societas Europea, European Economic Interest Groupings, Institutions, Associations and Foundations. Associations acquire legal personality upon voluntary registration in the Register of Associations. Foundations acquire legal personality upon registration in the Register of Foundations. Foundations cannot lawfully carry out activity until they are registered. These types of legal persons, their form and basic characteristics are prescribed under several laws, namely the Companies Law in the case of Companies, the Institutions Law, the Associations Law and the Foundations Law in the case of Institutions, Associations and Foundations, respectively. Societas Europea and European Economic Interest Groupings are regulated by EU legislation, namely Council Regulations (EC) No. 2157/2001 and No. 2137/85, respectively.

85. All companies, Societas Europea, European Interest Groupings and Institutions are required to be registered in the Court Register.

86. Since 2019, online company registration has been available using the START system for LLCs and SLLCs without requiring the services of a notary public.

87. Associations only acquire legal personality upon registration. Registration of associations are not mandatory, but these can be registered in the Register of Associations voluntary. The Register of Associations is maintained by the competent administrative body of the county or the City of Zagreb.

88. Foundations are set up by the formulation of the act of establishment and acquire legal personality and may perform their activities only upon being registered in the Register of Foundations. Foundations are required to be registered in the Register of Foundations maintained by the competent administrative body of the county or the City of Zagreb.

89. The majority of legal entities registered in Croatia have national BOs and have natural persons in the ownership structure. Out of the total number of registered legal entities in the BO Register, only 2.58% (4396) have a complex ownership structure with two or more legal entities in their ownership structure.

90. Associations, foundations, and institutions can be registered as non–profit organisations. NPOs are registered in the Register of NPOs on the basis of the application submitted to the MoF. Supervision of NPOs, in accordance with their competencies, is carried out by the MoJA, the MoF and TA. There are 42 782 registered NPOs.

**Table 1.3: Types of registered NPOs**

| Type of NPOs | Number |
|---|---|
| Associations | 39 391 |
| Foundations | 267 |
| Art organisations | 360 |
| Trade unions | 342 |
| Tourist boards | 310 |
| Institutions | 226 |

| Type of NPOs | Number |
|---|---|
| Chambers | 158 |
| Political parties | 155 |
| Foreign associations | 151 |
| Legal entities of Catholic Church | 30 |
| Cooperatives | 20 |
| Representative of national minorities | 19 |

| | |
|---|---|
| Religious communities | 171 |

| | |
|---|---|
| Other non–profit legal persons | 2 |
| Foreign Foundations | 12 |

91. Croatia introduced provisions on the establishment of the BO Register in the AMLTFL in 2019. It provides the legal basis for the setting up of a BO Registry. BO Registry should obtain and hold BO information of all legal persons and trusts and similar entities of foreign law. The BO Registry became operational on 1 January 2020 and is populated progressively. The BO Register is maintained by the Financial Agency (a public company) on behalf of the AMLO. Inspection over information kept with the BO Register is conducted by the TA.

**Table 1.4: Legal persons (data from the BO Register)**

| Legal form | Total Number | Basic ownership structure[102] | Beneficial Ownership geography | Description |
|---|---|---|---|---|
| LLC | 100610 | Only natural persons – 89,3%; Only legal persons – 7,29%; Natural and legal persons – 3,42% | Croatia – 88,22%<br>Italy – 1,72%<br>Slovenia – 1,40%<br>Germany – 1,10%<br>Austria – 0,97%<br>Bosnia and Hercegovina – 0,82%<br>Russia – 0,61%<br>United Kingdom – 0,47%<br>Hungary – 0,43%<br>Serbia – 0,42% | A LLC is a company of at least one or more director, one or more shareholder, and has one or more shares. Shareholders have limited liability for the obligations of the company. |
| SLLC | 32986 | Only natural persons – 98,7%; Only legal persons – 1,15; Natural and legal persons – 0,15% | | A SLLC is a company with a maximum of five members and one member of the management board. Shareholders have limited liability for the obligations of the company. The lowest amount of the company's share capital is HRK 10.00 |
| Institution | 1647 | Only natural persons – 67,03%; Only legal persons – 29,93%; Natural and legal persons – 3,04% | | An institution is a legal entity established for the permanent performance of activities of public interest. It acquires legal personality by registering in the Court Register. |
| Foreign Branch | 413 | Only legal persons – 100,00% | | The foreign branch is established based on a decision made by the competent body of the foreign company. The company acquires rights and obligations |

[102] The number refers to registered legal entities in the BO Register. The data provided for the Basic ownership structure are data on the founders of legal entities. For JSCs that are not listed on the stock exchange, data on first 10 control account holders are also available in the BO Register.

| | | | | |
|---|---|---|---|---|
| | | | | of branches' business operations. |
| General Partnership (GP) | 186 | Only natural persons – 94,62 %;<br>Only legal persons – 2,15%;<br>Natural and legal persons – 3,23% | | A general partnership is a company into which two or more persons are joined with the aim of continuous performance of activities under a common firm name, and each member of the company has unlimited and joint responsibility to creditors of the company with all his assets. |
| Limited Partnership (LP) | 45 | Only natural persons – 35,56 %;<br>Only legal persons – 26,67%;<br>Natural and legal persons – 37,78% | | A limited partnership is a company in which two or more persons are joined with the aim to permanently conduct activities under the common firm name, of whom at least one is subject to joint and unlimited liability for the obligations of the company with all his assets (general partner), and at least one is liable for obligations of the company up to the amount of the assets contributed into the company (limited partner). |
| Economic Interest Grouping | 28 | Only natural persons – 3,57%;<br>Only legal persons – 75,00%;<br>Natural and legal persons – 21,43% | | Economic interest grouping is a legal person formed by two or more natural or legal persons with the aim of facilitating and promoting the economic activities which form the objects of their business activities and to improve or increase their effect, but in such a way that legal person does not acquire profits for itself. |

| | | | | |
|---|---|---|---|---|
| Association of Institutions | 1 | Only legal persons – 100,00% | | Institutions may, with the consent of the founders, associate in an association of institutions. The association of institutions is a legal entity obliged to register with the Court Register. The provisions of the Institutions Act apply to the name, seat, activity and organisation of association of institutions. |
| Association | 33570 | No information is available | | Association is any form of free and voluntary association of several natural or legal persons who, in order to protect their benefits or advocate for the protection of human rights and freedoms, environmental and nature protection and sustainable development, and for humanitarian, social, cultural, educational, scientific, sports, health, technical, informational, professional or other beliefs and goals that are not in conflict with the Croatian Constitution and the law, and without the intention of gaining profit or other economically assessable benefits. |
| Foundation | 164 | | | Foundation is a non–profit legal entity without members. It is an asset intended to permanently serve the realisation of some public benefit or charitable purpose. |
| JSC | 748 | | | JSC is a company, the equity capital of which consists of the total |

| | | | | |
|---|---|---|---|---|
| | | | | sum of the nominal value of equity capital stock and the shares (stock) of which may be publicly tradable objects |
| Sport JSC | 9 | | | No information available. |

92. Croatia is not a signatory to the Hague Convention on Laws Applicable to Trusts and their Recognition. There are no trusts governed under the laws of Croatia. However, trusts and similar legal arrangements set up under foreign laws may still carry out financial and other activities in Croatia. Moreover, natural or legal persons in Croatia may also provide trustee services and are considered REs and subject to AML/CFT obligations under the AMLTFL when they do so.

93. The BO Register should contain information on the trust/similar legal arrangements and the BO of the trust/similar legal arrangements (unless it is registered in an EU Member State):

– whose trustee or a person performing equivalent or similar functions has residence or seat in the Republic of Croatia;

– whose trustee or a person performing equivalent or similar functions doesn't have residence or seat in the Republic of Croatia nor in another Member State but who on behalf of the trust or similar entity established under a foreign law acquires a real estate in the Republic of Croatia or establishes a business relationship with the RE.

### Table 1.5: Legal arrangements

| Type | Total Number | Type of provided services | Beneficial Ownership geography |
|---|---|---|---|
| Trust[103] | N/A | N/A | N/A |
| | | | |
| Other | – | – | – |

94. There is a concept of a pooled investment vehicle, a type of collective investment fund that can be a UCITS[104], an AIF[105] or a pension fund (voluntary or mandatory)[106] in Croatia, which do not have legal personality. There is no consistent regulatory approach to these formations throughout the EU Member States[107]. In some countries, these are recognised to be legal arrangements, and in others, as also Croatia, these are recognised as a financial product[108]. Respectively, the assessment team treated these as a type of financial product when discussing with the private sector and the competent authorities.

[103] One company registered in Croatia as LLC provides fiduciary services, and notaries and lawyers provide trust and company services.
[104] See definition of investment fund, UCITS fund and open–ended investment fund in Article 4 of Law On Open Investment Funds With Public Offer.
[105] See definitions of open–end AIF and closed ended AIF without legal personality – Article 4(4) and (5)(b) of Law on Alternative Investment Funds.
[106] See definition of voluntary pension fund without legal personality – Article 3(3) Law on voluntary pension funds.
[107] EUR–Lex – 52020DC0560 – EN – EUR–Lex (europa.eu)
[108] See Part Three Relationship between AIFM, AIF without legal personality and investors Law on Alternative Investment Funds and Part Three relationship between management company, UCITS fund and Investors. Section II Fund Membership Law on voluntary pension funds.

### *1.4.6. Supervisory arrangements*

95. There are four AML/CFT supervisors in Croatia supervising all REs. The basic powers and responsibilities of these supervisors are set out in the AML/CFT Act. There are no licensing requirements currently set for accountants, TCSPs, VASPs, DPMS and art objects and antiquities, or auctions, but these are supervised for the AML/CFT purposes by the Financial Inspectorate and the CFSSA.

96. Supervisory authorities co–operate and coordinate among themselves and with the AMLO on the basis of interagency bilateral MoUs and on the IIWG supervisory sub–group platform.

**Table 1.6: Supervision of Financial Institutions and VASPs**

| Type of FI | AML/CFT Supervisor | Licensing Body (Market Entry) |
|---|---|---|
| Banks | CNB | CNB |
| Savings banks | CNB | CNB |
| Housing savings banks | CNB | CNB |
| Credit unions | CNB | CNB |
| Payment institutions | CNB | CNB |
| Electronic money institutions | CNB | CNB |
| Life insurance companies | CFSSA | CFSSA |
| Insurance | CFSSA | CFSSA |
| Investment funds management companies | CFSSA | CFSSA |
| Investment funds (having a legal status and internal management) | CFSSA | CFSSA |
| Pension companies managing voluntary pension funds | CFSSA | CFSSA |
| Pension insurance companies | CFSSA | CFSSA |
| Investment firms | CFSSA | CFSSA |
| Leasing companies | CFSSA | CFSSA |
| Factoring companies | CFSSA | CFSSA |
| Legal and natural persons providing exchange services between virtual currencies and fiat currencies and custodian wallet services (VASPs) | CFSSA | There is no licensing requirement, but notification should be filed with CFSSA |
| Authorised Exchange offices | Financial Inspectorate | CNB |
| MVTSs | Financial Inspectorate | CNB for money remittance providers<br>HAKOM[109] for the Croatian Post |
| Croatian Banks of Reconstruction and Development | Financial Inspectorate | established on the basis of the Act on Croatian Bank for Reconstruction and Development |
| Consumer credit service providers | Financial Inspectorate | MoF |

[109] Croatian Regulatory Authority for Network Industries

### Table 1.7: Supervision of DNFBPs

| Type of DNFBPs | AML/CFT Supervisor | Licensing Body (Market Entry) |
|---|---|---|
| Lawyers | Financial Inspectorate | Croatian Bar Association |
| Notaries public | Financial Inspectorate | Croatian Notaries Chamber |
| Accountants | Financial Inspectorate | No license is required to enter the market |
| Tax advisors | Financial Inspectorate | Croatian Association of Tax Advisors |
| Auditors | Financial Inspectorate | MoF |
| Real estate brokers | Financial Inspectorate | Croatian Chamber of Commerce |
| Organisers of game of chance:<br>– Lottery games<br>– Casino games<br>– Betting games<br>– Gambling on slot machines<br>– Online gambling | TA | MoF, TA |
| Dealers in precious metals and in precious stones | Financial Inspectorate | No license is required to enter the market |
| Dealers in art objects and antiquities, auctions | Financial Inspectorate | No license is required to enter the market |
| Trusts and company service providers | Financial Inspectorate | No license is required to enter the market |

97. All legal or natural persons carrying out a registered activity in Croatia are prohibited from receiving/making payments in cash in the amount of EUR 10 000 or more. TA is the designated supervisory authority for compliance with this rule.

#### *1.4.7. International co–operation*

98. Croatia has adequate mechanisms, including an extensive network of multilateral treaties, to provide and seek the broadest range of mutual legal assistance (MLA) and extradition in relation to ML, associated predicate offences (except for fiscal offences) and TF. This especially applies to co–operation with EU–Member States. Most of the foreign co–operation in Croatia is conducted through the SAO via the dedicated mechanisms provided for the EU Member States (ILA and EIO). The MoJA, the central authority for exchange of MLA requests with foreign counterparts, mostly deals with co–operation with non–EU Member States. Croatia has arrangements (MoUs) with its non–EU Member States neighbour countries with whom it co–operates most frequently. LEAs make use of direct co–operation mechanisms. Supervisory authorities, when necessary, may benefit from various EU mechanisms and membership in international organisations, providing access to foreign counterparts. The AMLO has all the necessary tools and mechanisms and actively co–operates with its foreign counterparts.

# 2. NATIONAL AML/CFT POLICIES AND COORDINATION

## 2.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 1***

a) Croatia has made efforts to develop its understanding of ML/TF risks through two NRAs conducted in 2016 and 2020. The second NRA does not demonstrate an increased level of understanding from the first one, and it did not lead to a more sophisticated understanding and response to ML/TF risks. The CNB's and the Financial Inspectorate's sectoral assessments and the AMLO's typologies reports contributed to the understanding of some specific ML risks.

b) The understanding of ML risks is uneven across the Croatian authorities. The supervisors' understanding ranges from comprehensive to inadequate in the order from CNB, Financial Inspectorate, CFSSA to TA. Amongst the LEAs, SAO and SIA level of ML risk understanding was mostly identical and reflective of the NRA findings. The AMLO's risk understanding was broader than the NRA suggests, regarding observed trends and typologies. The TF risks understanding did not prove to be sufficient across all authorities, with the CNB and the Financial Inspectorate demonstrating a comparably better understanding at a sectoral level.

c) Overall, understanding of ML/TF risks was affected by several shortcomings related to identification and assessment of risks: conclusions are based on the empirical knowledge due to the systemic lack of quantitative data; data on undetected criminality is not explored; STRs and other financial intelligence and a range of foreign co–operation requests are not systematically explored.

d) The authorities could mainly describe the top three ML threats in terms of the predicate offences but could not explain them in terms of the ML risks. There was overall awareness of various risks in the system, e.g., organised crime, use of cash, cross–border risks, trade–based ML, risks related to VA and VASPs but, deeper understanding was yet to be developed.

e) The impact of certain vulnerabilities on the risk environment of the country was not demonstrated to be understood: e.g., the gap in knowledge of ML and TF offences, systematic delays in judicial proceedings, shortage of human resources, issues with maintaining criminal statistics, etc.

f) All competent authorities explained the low TF risk in Croatia by the absence of terrorist acts in the country. They could not explain in a consistent manner how conclusions on a decrease of the TF risk from 2016 to the 2020 NRA was reached. Authorities did not demonstrate considering TF risks from the OCG, migrant smuggling, remaining stock of weapons, financing of the FTF family members.

g) Croatia has developed three strategic documents that, while not informed by the ML/TF risks, are aimed at setting policy objectives, in particular, in the areas of suppression of corruption and prevention of TF. The Government of Croatia also adopted two Action Plans for mitigation of ML/TF risks detected on the basis of the 2016 and 2020 NRAs. The latter are described by Croatia as representing a national AML/CFT policy, which raises doubts on the basis of the substance of these: (i) the Action Plans are separate actions prescribed to respective competent authorities, with no overall strategic plan for the IIWG; (ii) it is not apparent how the set actions are linked to and will mitigate the higher ML/TF risks of Croatia.

h) Exemptions for external accountants and VASPs and a statutory exemption are neither supported by risk assessment results, nor do they occur in strictly limited and justified circumstances. Simplified and enhanced measures are applied in line with identified risks in most cases. Croatia has introduced some additional specific requirements for REs that take into account the 2016 NRA findings.

i) In a number of areas authorities focus on addressing key threats and vulnerabilities, but actions lack sufficient focus on combating ML/TF in line with the identified risks. Among authorities, the supervisory objectives and activities of the CNB and Financial Inspectorate are informed by the ML risks to greater extent than that of the CFSSA. The TA's objectives are fully shaped around the tax revenue/evasion, which is a positive practice to fight tax evasion as a major threat in the country but has very little effect in their role of a supervisor. The LEAs and AMLO are acting driven by priorities set according to their individual observations, limited to their own area of operational activity.

j) Support at the policy–making level is not demonstrated enough when it comes to strategic coordination of combating ML/TF. At an operational level, competent authorities demonstrated good co–operation and co–ordination on ML/TF issues, but this needs to be further extended when it comes to interaction between LEAs and licensing and supervisory authorities. The co–operation and co–ordination on the PF matters is to be developed further.

k) The private sector was made aware of the NRA outcomes.

***Recommended Actions***

***Immediate Outcome 1***

a) Croatia should strengthen its high level policy coordination in combating ML and TF by: (i) introducing policymakers into the AML/CFT coordination mechanism – IIWG; (ii) articulating the national AML/CFT policies, objectives and activities in a strategic framework, and providing with necessary resources (budgetary and human); (iii) providing the IIWG with necessary powers for implementation of AML/CFT policies, objectives and activities commensurate to ML/TF risks; (iv) ensuring regular monitoring of implementation of respective AML/CFT policies, objectives and activities by the IIWG, and

assessment of the impact on the ML/TF risks in Croatia. The co–operation and co–ordination on the PF matters should be developed further.

b) Croatia should enhance its ML/TF risk understanding, deepening it in the areas currently covered in the NRA and further expanding identification and assessment of risks related to ML (organised crime, use of cash cross–border risks, trade–based ML, risks related to VA and VASPs) and TF (OCG, migrant smuggling, remaining stock of weapons, financing of the FTF family members). Croatia should ensure the use of comprehensive quantitative data (actual crime, undetected criminality, STRs, other financial intelligence, foreign co–operation requests, including MLA and other forms of co–operation), in addition to its empirical knowledge.

c) Croatia should reconsider currently applied exemptions (with respect to external accountants, VASPs, and statutory exemption from the AMLTFL when providing financial services as a secondary activity) and ensure that these are allowed only with respect to some of the AML/CFT requirements and occur in strictly limited and justified instances where there are proven low risks.

d) Croatia should set mechanisms for the communication between LEAs and all licensing and supervising authorities: (a) for sharing with licensing and supervising authorities in instances when authorised/licensed persons are suspected in criminal matters, enabling them to take timely and adequate measures; (b) for sharing with LEAs the supervisory expertise when the REs are abused or concerned in criminal cases.

e) When developing NRA Action Plan, Croatia should ensure that the actions are directed to mitigation of Croatia's AML/CFT risks, actions are granular, measurable, have concrete timeframes for implementation and set specific goals and outcomes that are achievable and measurable.

f) Croatia should continue taking measures to reduce the use of cash. Targeted actions are required in the real estate sector regarding cash transactions by natural persons.

## 2.2. Immediate Outcome 1 (Risk, Policy and Coordination)

### *2.2.1. Country's understanding of its ML/TF risks*

99. Croatia has a varied understanding of its ML risks. Understanding of TF risks is not sufficient. This risk understanding was developed mostly on the basis of the two NRAs conducted in 2016 and 2020, into which the authorities put significant efforts. Nevertheless, the second NRA does not demonstrate an increased level of understanding from the first one, and it did not lead to a more sophisticated understanding and response to ML/TF risks.

100. Croatia relied upon the World Bank tool when assessing the ML/TF risks. Some inflexible and inadequate application of certain aspects of the methodology affected findings of Croatia in 2020 (see R.1).

101. These two NRA reports benefited from input from the majority of key AML/CFT authorities in the country. The MoJA, Corruption Prevention Sector was not involved in the assessment, and

the NRA did not benefit from their input. The private sector participation varied. Major market players (3 largest banks), securities and insurance sectors, representatives of SRBs (notaries, lawyers, real estate agents and accountants) took part in person. Other FIs and DNFBPs participated through questionnaires.

102. Across all four supervisory authorities, the understanding of ML risks varies, the strongest being demonstrated by the CNB and weakest by the TA. The CNB demonstrated a comprehensive understanding of the ML risks of the sectors it supervises. This understanding was primarily developed through the annual sectoral risk assessments of the supervised sectors. The Financial Inspectorate displayed a more in–depth understanding of the vulnerabilities in its supervised sectors than was evidenced in the NRA. The CFSSA demonstrated it understood the ML risks identified within the NRA and relied solely on these, except for when it comes to the VASP sector vulnerabilities. The TA was unable to adequately articulate its understanding of the ML risks of the supervised sector.

103. Amongst LEAs, SAO and SIA level of ML risk understanding was mostly identical. The AMLO's risk understanding was broader than the NRA suggests, especially through its observed trends and typologies.

104. The TF risks understanding did not prove to be sufficient across all authorities. Most of the authorities were overly reliant on the NRA analysis, while the CNB and the Financial Inspectorate did so to a lesser extent, giving consideration to risks at a sectoral level (see IO.3). Respectively, the TF understanding was affected by several shortcomings related to identification and assessment of the TF risks in Croatia.

*ML risk understanding*

105. Understanding of ML threats by most of the Croatian authorities was focused on the three main threats, such as tax evasion, drug trafficking and corruption. While these three threats remain through two cycles of evaluations conducted by Croatia in 2016 and 2020, respectively, corruption used to be the number one threat in 2016. No rationale has been provided for the reprioritisation of these threats. Fraud – the most frequent predicate offence to ML detected by the authorities was given less prominence.

106. The authorities could mainly describe the threats in terms of the predicate offences. They could not always demonstrate their understanding as to how these threats could be explained in terms of the ML risks. This was also evidenced through the low number or non–existence of ML investigations, prosecutions and convictions related to these three major threats.

107. With respect to tax evasion threat, among the authorities, the TA has demonstrated knowledge of methods and techniques used to generate and move illicit funds with respect to tax evasion (e.g., VAT fraud, use of strawman, shell companies, and involvement of criminal associations). The TA could also explain the occurrence of ML associated with the tax crime in some limited instances, but the LEAs could not. The AMLO could elaborate on the ML risks emanating from the tax crime on the basis of knowledge formed through the observed trends and typologies. Nevertheless, understanding of the significance of the threat emanating from this crime, a reliable estimate on the amounts of involved proceeds of crime, and the vulnerabilities that create favourable conditions for this type of criminality are yet to be developed.

108. As concerns the understanding of drug trafficking threats, it is mostly shaped around the recognition of the geographical exposure of Croatia. Croatia remains a transit point for illegal drugs trafficked along traditional Balkan smuggling routes. Croatia is also a drug manufacturing

country of some relatively small volumes mainly targeting the domestic market (see also Chapter 1). Croatia recognises the fact of involvement of criminal associations and the prevalence of the use of cash in dealing with drugs. Nevertheless, these factors are considered in the framework of the predicate offence and the authorities suggested that there were never ML investigations conducted associated with drug trafficking and could respectively provide no clear explanation as to how the proceeds of drug trafficking would be laundered, which types of financial or non–financial services would be used and hence, what would be the ML risks, specifically.

109. With respect to corruption as an ML threat, similar to drug trafficking, authorities could elaborate on the predicate offence itself. Corruption cases dealt with by the LEAs include high–ranking individuals, including a former prime minister, these being in a majority of cases related to abuse of a state–owned or other public property. In addition, the authorities indicated cases of corruption in the private sector, including the football sector. Criminal association is also being highlighted as a common feature of corruption. Concealment of the illicit funds, use of financial institutions for withdrawing funds in cash or transfer of funds using internet banking services were explained to be the common methods of committing corruption. Croatia nevertheless did not present or describe ML cases related to corruption that could confirm the authorities' understanding of ML risks in this area. In addition, the MoJA – the leading authority in the corruption prevention sector, who were not involved in the NRA, could discuss the level of corruption in the country only in terms of the results of the corruption perception survey (e.g., Eurobarometer surveys on corruption), noting that the perception is higher rather than the actual corruption risk.

110. Organised crime is not considered by the Croatian authorities among the top threats to ML despite organised criminal groups frequently featuring in a range of criminal offences, such as the ones indicated above and also, human trafficking and smuggling of goods (cigarettes, tobacco, arms, ammunition, alcohol and the protected animal species), etc. Authorities suggested that the Police carry out regular assessment of ML risks within the scope of "Serious and Organised Crime Threat Assessment for Croatia" analysis. Nevertheless, on–site, authorities did not demonstrate how this analysis could contribute to their understanding of the ML risks. The full document was also not made available to the assessment team to draw conclusions on the significance of this phenomenon in the criminal landscape of the country and the volume of proceeds of crime generated and controlled by these structures.

111. Use of cash features in Croatia as the most common instrument of crime. The authorities demonstrated awareness of several cases, including of a transnational nature that involves cash. Croatia has introduced various thresholds for operation, identification and reporting of cash both following the EU regulatory framework and their own observations. Nevertheless, the continuous nature and gravity of the consequences of use of cash in the country by criminals point out the need for further systemic analysis of this phenomenon to deepen the understanding of the vulnerabilities in this sector and to develop an adequate response for limiting the use of cash in the county.

112. Cash is a common medium used in drug trafficking. This, in many instances, is explained by the authorities to prevent them from evidencing the link between the cash and the drugs, thus hindering effective investigation and deprivation of criminals of funds. This example highlights the need for the authorities' deeper understanding of the gap in knowledge (understanding of ML) for investigating such cases. Proceeds of crime in cash are also frequently used for purchase of real estate, including luxury property on the Croatian coastline. Setting up legal persons in Croatia, transferring funds on the account that follows cash withdrawal is a scheme that had been

well known to the authorities for many years. While some preventative measures are established, such as proof of a link with the country when establishing a customer relationship with a financial institution, there is a need for further deepening the understanding of authorities about the associated vulnerabilities, e.g., mechanisms of setting up of companies in Croatia (see IO.5), to develop a more robust response. While the AMLO conducted analysis of the CTRs for 2018 and 2019 as reflected in its annual report, these were not taken into consideration at a national level to further develop the findings. This analysis contains valuable data on the trends in the annual use of cash in transactions and indication of the citizenship of the persons most frequently using the cash. Further analysis, nevertheless, is needed to understand the origin and rationale for use of cash, especially by foreigners coming from neighbouring countries, with the purpose of detecting potential criminal patterns.

113. There was not sufficient focus on cross border movement of cash and goods. A list of raw data is available to authorities about the volume of cash and goods passing through the customs controls. There is no analysis or understanding demonstrated of proportionality of these transportations with international trade and the financial flows to identify potential transfers with no link to actual business, which could indicate the risk of trade–based ML.

114. As concerns the risks emerging from virtual asset activities and the activities or operations of VASPs, currently, Croatia demonstrated it is taking its first steps in developing its understanding of vulnerabilities of this sector. This was demonstrated through a basic analysis of the market's economic metrics and an observation of the legislation, but broader appreciation of the risks in the sector is yet to be developed. There is a need to develop the understanding of the ML risks in the sector, including through increasing the knowledge about the size and participants of the sector, the full scope of the offered services, the type of criminality that makes use of the virtual assets in Croatia.

115. Croatia reached conclusions on the main three threats on the basis of estimated frequency and volume of generated proceeds. This turned to be based on the empirical knowledge of the authorities, as no figures for the crime rate and generated proceeds were made available to the AT. In addition, this conclusion is merely based on the authorities' observations of the actual crime, and does not take into consideration the undetected criminality, STRs, other financial intelligence, foreign co–operation requests, including MLA and other forms of co–operation. The manner of collecting judicial statistics and information on confiscated assets also hampers the authorities' ability to accurately identify the frequency of crime and volume of generated proceeds, including cross–border illicit flows (be it outwards or inwards). Most of these vulnerabilities are recognised by the authorities.

116. In the 2020 NRA, Croatia highlighted a very important vulnerability that seriously affects the ML risk appreciation of the authorities. It is a restrictive interpretation of the ML offence confirmed by two judgements of the Supreme Court of Croatia[110] (see analysis of judgements under IO.7). While the authorities confirmed that these two judgements do not set a precedent for prosecutors and judges, the latter nevertheless agreed with the Supreme Court judgements. This widely explains the lost opportunities – absence or low number of ML investigations that should have been carried out on the basis of the above–mentioned predicate offences. Such dissonance between the NRA findings and the position expressed by the authorities questions

[110] The Supreme Court of the Republic of Croatia, I Kž 625/13–6 of 28 May 2015, I Kž 560/16–4 of 28 November 2016.

Croatia's understanding of this fundamental vulnerability which has material consequences and seriously impacts the ML risk understanding in the country.

117. With respect to the judicial proceedings, one of the other long–standing serious vulnerabilities recognised by the Croatian authorities are the undue delays in court criminal proceedings (e.g., lasting for more than 10 years to achieve a conviction). Another issue is the undue delay in confirmation of indictments by the court, which leads to the release of seized assets (see IO.7). It is understood that the cause for these delays is due to procedural matters. The authorities, nevertheless, did not display consideration of other possible factors contributing to such issues in the judicial proceedings, e.g., corruption in the judicial system. The losses from such delays were not analysed in a systemic manner to assess the consequences of this vulnerability.

118. Another important vulnerability of a systemic nature that affects nearly all key structures involved in the AML/CFT system of the country is a shortage of human resources, which is another long–standing issue present in SAO, AMLO and some supervisory authorities to a varying extent. This shortage prevents effective implementation of criminal proceedings, detection and use of financial intelligence and application of supervisory measures. The issue of poor resourcing of SAO is a fact also recognised in the international reports highlighting the shortage of specialised investigators for dealing with financial crime (see IO.7). Considering that the AMLO plays an important role in detection of ML and associated predicate offences and supplying the LEAs with important financial intelligence, systemic staff shortage of around 50%–60% in AMLO, including the shortage of analysts, speaks to the lost opportunities over the past years (see IO.6). As further described in the report (see IO 3), such a shortage also affects the implementation of the RBA in supervision and considerations of the types and cycles of inspection. The authorities did not demonstrate that they have measured the bearing of this issue on the vulnerability of the system and consequences that this has on the risk environment of the country.

*TF risk understanding*

119. When discussing the TF phenomenon on–site, all the stakeholders' understanding of TF risks was linked to the absence of terrorist attacks in Croatia and the assessment of TF risk as low in the NRA with little consideration of potential or inherent TF risks. There was a decrease[111] in the TF risk appreciation of the authorities in the period falling under the assessment (from medium low in 2016 NRA to low in 2020 NRA), which was not consistently explained by the authorities (across authorities different reasoning was provided, changing it also after the on–site) (see also IO.9).

120. The authorities did not demonstrate consolidating and conducting a systematic analysis of TF risks using all available information, including STRs, MLA, foreign co–operation and available intelligence, and drawing a holistic picture. They did not also demonstrate considering the TF risks that specifically can be emanating from the OCG, migrant smuggling, remaining stock of weapons, financing of the FTF family members (see also IO9).

121. The appreciation of the TF risk in Croatia is also affected by a gap in knowledge. When discussing TF risk, authorities were commonly associating this offence with provision of financial resources, focusing on analysis of financial transactions or use of ATM to withdraw cash. However, there is a lack of consideration that TF can be committed by providing other funds and

[111] The 2016 NRA identified a medium–low TF risk, but the 2020 NRA estimated the TF risk as low.

assets. In addition, the provision of small amounts of funds to a FTF family member was not considered as a potential TF offence (see also IO.9).

122. Croatia made efforts to conduct an assessment of risks in the NPO sector. The NPO sector was considered within the scope of the two NRAs conducted in 2016 (subject to ML vulnerabilities in the sector), 2020 (as a variable for assessment of the Country's TF vulnerabilities), and a thematic analysis by the Financial Inspectorate. None of these exercises led to the identification of a subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse by virtue of their characteristics. Authorities suggested analysing the number of active and passive NPOs and their outgoing and incoming transactions and other data to assess their TF exposure. This, nevertheless, does not seem sufficient to understand the potential risks that can arise from the geographical and operational context of the NPO activities, including when raising funds, providing various types of support in the scope of doing "good works", beneficiaries of the NPO activities and their possible affiliation with terrorist groups. The understanding of the country also does not seem to focus on the vulnerabilities in the monitoring of the NPO activities, which would not allow active detection of a wrong–doing one (see also IO.10).

123. When discussing the vulnerabilities present in the system in the context of the TF, it appeared that the authorities do not differentiate these from the ones identified for ML. The AT deems that this indicates the need for deepening the understanding of the vulnerabilities that would be typical for the TF. One of the most important vulnerabilities in the system – shortage of human resources, as described above is also relevant here.

124. As the evaluation process undertaken by the AT moved towards its conclusion, Croatia provided some case examples having links with TF offence that were dealt with by various authorities. Subsequent information provided on the TF occurrence in the country raises questions in the minds of the AT about the extent to which the TF risk appreciation displayed by the authorities is accurate.

### *2.2.2. National policies to address identified ML/TF risks*

125. There are three strategic documents in Croatia that are aimed at setting policy objectives, in particular, in the area of suppression of corruption and prevention of financing of terrorism. These are, respectively, the 2015–2020 Anti–Corruption Strategy, the 2015 National Strategy for the Prevention and Suppression of Terrorism and the 2017 National Security Strategy of the Republic of Croatia. In addition to this, Croatia has also adopted two Action Plans developed on the basis of the 2016 and 2020 NRAs, aimed at implementing measures to address identified ML/TF risks.

126. The 2015–2020 Anti–Corruption Strategy reflects the political commitment of Croatia to the fight against corruption and creation of systematic solutions for efficient suppression of corruption[112]. This Strategy is the fourth cycle of the anti–corruption measures implemented by the country (the first being developed in 2002) and is focused on the prevention of corruption through detection of corruption risks and improvement of the legislative and institutional framework. This document acknowledges the membership of Croatia in "Partnership for Open Government" and strives to address recommendations given to the country within the scope of

[112] 2015–2020 Anti–Corruption Strategy, p.3

the Anti–Corruption Report of the European Commission and the 4th round evaluation of GRECO in 2014.

127. While not developed on the basis of the NRA outcomes, this document, nevertheless, is in line with the findings of the two risk assessments that consider corruption to be within the range of the top three ML threats. According to the 2015–2020 Anti–Corruption Strategy, Croatia concluded to be necessary to anticipate more robust mechanisms of interinstitutional co–operation of the Tax Authority for the suppression of corruption, based on the development of standardised procedures and the advancement of technical facilities for the exchange of information with other bodies (SAO, MoI, Office for Money Laundering Prevention). The respective action to be taken is described as establishing automated processing of transactions and individuals towards the acceleration of operating processes of the AMLO. The report about the implementation of the 2015–2020 Anti–Corruption Strategy confirmed the accomplishment of the action. A new Strategy on the Prevention of Corruption for 2021–2030 is in the public consultation process.

128. Another strategic document adopted by Croatia, is the 2015 National Strategy for the Prevention and Suppression of Terrorism. It is also not supported by the NRA findings as preceded the events. This Strategy, nevertheless, reflects not only on combating terrorism but acknowledges the necessity for also tackling TF. In particular, one of the measures to take is the prevention of financing, the collection of the means or any kind of assistance to terrorist organisations or persons thought to be connected with terrorism. This should be achieved through the strengthening of the implementation of financial investigations through the swift exchange of relevant data at national and international levels aimed at the use of security measures to seize proceeds of crime (freezing) and to seize any form of proceeds of crime from natural and legal persons connected with terrorist activities.

129. Another strategy that was not driven by NRA is the 2017 National Security Strategy of the Republic of Croatia and the 2019 Report on the Implementation of the National Security Strategy. These, nevertheless, have elements that are largely complementary to the NRA, for example, a commitment to combatting threats of corruption and terrorism.

130. On the basis of the two NRAs from 2016 and 2020, the Government of Croatia adopted two Action Plans for mitigation of the detected risks. These are described by Croatia as representing the national AML/CFT policy. Taking into consideration the substance of the set actions, and that these Action Plans were rather separate actions prescribed to respective competent authorities, with no overall strategic plan for the IIWG, the AT considers that these do not suggest setting a national policy.

131. The fact that through the NRA, Croatia has not identified certain risks and certain risks are not understood to a significant extent have a bearing on the Action Plans developed on the basis of the two NRAs. Nevertheless, the 2016 Action Plan compared with the one from 2020 was detailed and inclusive. The Action Plan from 2016 NRA consisted of 21 points. All the actions were set to be accomplished by the end of 2017. It reflected on several vulnerabilities detected in the NRA. Many of the measures, especially in the supervisory field and the area of strengthening implementation of preventative measures, were accomplished within the set schedule, and others were in progress. Some actions, such as insufficient capacities of the SAO and financial investigators remained unachieved up to now, despite the steps being taken by the authorities. The effect of the implementation of measures, however, was not reflected in the 2020 NRA to assess and confirm the impact on mitigation of ML/TF risks.

132. The 2020 NRA Action Plan included 13 unprioritised action points which were vague, unmeasurable, lacked granularity and had no outcomes or goals specified and it is not apparent how they relate to the higher risks identified in the 2020 NRA. All the actions were set to be accomplished before the end of 2021 the latest. Cumulatively these actions were focused on: (i) enhancing the capacities of the AML/CFT authorities by conducting continuous training and education, strengthening administrative capacities, enhancing co–operation and communication; (ii) increasing AML/CFT supervision (by CFSSA); (iii) providing regular feedback to REs (by AMLO); (iv) collecting information from DNFBPs for risk assessment purposes (Financial Inspectorate and TA). The 2020 Action plan is non–contentious and does not tackle the fundamental issues raised across the two risk assessments, such as lack of successful ML/TF prosecutions, lack of measures regarding detection and confiscation, the need for further training of the judiciary, law enforcement and investigators, inability to secure an adequate number of personnel in the Financial Inspectorate, addressing barriers to recruitment of financial investigators, etc.

133. The following analysis demonstrates unsatisfactory high–level policy co–ordination in relation to national responses to ML/TF risks. The competent authorities were undertaking actions on an individual basis that were compatible with but not driven by the NRA findings. These were based on their own assessments of what is required to mitigate the risks. These activities are not undertaken in any nationally coordinated way. A noticeable example is that the TA split its capacity into tax investigations and economic crime/AML investigations to improve its efficiency and performance. This was an important undertaking that was not driven by the NRA Action Plan, but rather by the own initiative of the TA.

134. Another example of the unsatisfactory support at the policymaking level co–ordination in relation to national responses to ML/TF risks is the lack of systemic Government support for implementation of the Action Plans developed on the basis of the two NRAs. Authorities were provided with no extra resources, and each relevant body was left to seek resources themselves as part of their own annual budgeting, which did not prove to be successful, as also reflected in the 2018 Report on Implementation of the 2016 Action Plan.

135. The AT considers that the major contributing factor to the above–described issue is the fact that despite IIWG being composed of highly dedicated professionals, the latter are not high–level officials vested with prominent powers for ensuring systemic support to implementation of the national measures for combating ML/TF in Croatia. Therefore, the AT deems that commitment at the policymaking level to address AML/CFT issues in Croatia requires further enhancement.

### *2.2.3. Exemptions, enhanced and simplified measures*

*Exemptions*

136. The justification for the exemptions outlined below does not properly apply FATF Recommendations as none of the scenarios are low risk, and it is not evidenced that they occur in strictly limited and justified circumstances.

137. There are two types of REs that are not properly designated and hence the FATF Recommendations do not apply to them: external accountants (with respect to activities as per R.22) and VASPs, except for the ones engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers (with respect to other activities as per R.15 and VASP definition). These exemptions are not supported by the conducted risk assessments. The sectors are deemed to be of a moderated ML/TF vulnerability level. The current exemptions

are the reflection of direct implementation of the EU regulatory with no further consideration of the scope covered by the FATF Standards.

138. There is a statutory exemption set out for REs from application of the AMLTFL when providing financial services, which relates to secondary financial activity, for example, where hotels or gas stations act as exchange offices. These REs are required to notify the Financial Inspectorate that this exemption is being relied on and that the conditions are fulfilled. Authorities suggested that there were 1188 authorised exchange offices at the end of 2020, and for only 200, it is their predominant activity. Out of these, only 3 REs have relied on this exemption over the last 3 years. While the exchange office sector's ML/TF vulnerabilities are estimated at the level of Medium in the NRA, the Financial Inspectorate has individually assessed these 3 REs as being at a low level of risk. Croatia has presented statistical data on the turnover of these 3 entities for 2019–2020. This all proves that the exemption is applied in limited instances. But the exemption is applied not from some requirements under AMLTFL but from all. Therefore, the AT could not confirm that the applied exception is in line with the FATF Standards.

*Enhanced Measures*

139. Articles 44 to 53 of the AMLTFL list scenarios when REs are obliged to apply EDD measures. Both REs and the supervisory authorities demonstrated an understanding of when EDD needed to be applied and what needed to be done. In addition, despite no specific countries being designated as posing a higher risk specifically to Croatia in the NRA, some REs demonstrated that the NRA led them to designate higher risk countries on the basis of one of the AMLO's typologies. Further, EDD is applied when faced with individuals that may be illegal immigrants, where also proof of permission to reside in Croatia was obtained (see also IO.4)

*Specific Measures*

140. In 2018, in response to risks highlighted in the 2016 NRA, Croatia adopted specific measures to prevent misuse of cash and mitigate ML threats, such as corruption. These measures are respectively: (i) reducing the CDD threshold for authorised exchange offices and DPMS to HRK 15 000 (EUR 2 000); (ii) requiring that REs collect information on the source of funds when conducting a cash transaction in the amount of HRK 200 000 (EUR 27 000) and more; and (iii) expanding the definition of PEPs to include municipality prefects, mayors, county prefects and their deputies elected on the basis of the Act regulating local elections in Croatia[113]. The 2020 NRA recommends that the CDD threshold be further reduced for authorised exchange offices, which is not included in the 2020 NRA Action Plan.

*Simplified Measures*

141. Indicators of potentially lower risk scenarios are included in the AMLTFL (Art.14(2–5) for customer; geographic; and products, services, transactions or delivery channels. There is a conditional limited exemption in relation to the E–money sector. They are permitted not to apply certain CDD requirements based on an appropriate risk assessment indicating that the risk is low provided that certain mitigating conditions are met (e.g., limited re–loadability, maximum limit of HRK equivalent to 150 Euro, use only in Croatia and absence of anonymity) (AMLTFL, Art.18). The exemption has been directly transposed from the 5th AML Directive. However, the NRA concludes that the risk posed by E–money providers is Medium in Croatia. Authorities clarified that NRA analysed the total business of E–money institutions, not focusing on the electronic

[113] Reasoning for adoption of the AMLTFL, Ministry of Finance, 2017

money products only. There are only five E–money institutions assessed by the NRA (two credit card issuers and three mobile operators whose primary activity is not the issuance of electronic money). For all of these five entities issuance of electronic money is a secondary activity. Analysis of electronic money institution´s business showed that in the period observed by the NRA (2015–2018) the value of transactions made by E–money institutions ranged between EUR 1 622 165 in 2015 to EUR 2 155 815 in 2018. The highest recorded average value of e–money transaction scores 0,67 EUR (data for 2018). The assessment team therefore considers that in the light of the materiality of the issue it does not have any serious bearing on the rating for IO.1.

### *2.2.4. Objectives and activities of competent authorities*

142. There are a number of areas where authorities focus on addressing key threats and vulnerabilities, but these activities lack sufficiently targeted focus on combating ML and TF. The LEAs and AMLO were acting driven by priorities set according to their individual observations, limited to their own area of operational activity. The supervisory objectives and activities of the CNB and Financial Inspectorate were informed by the ML risks identified in the NRA and also through their own efforts. The CFSSA activities were driven by the findings of the NRA. The objectives and activities of the TA were fully shaped around the tax revenue/evasion matters, which was a positive practice to fight the tax evasion as a major threat in the country but did have very little effect in their role as a supervisor of a gambling sector. With regard to the TF risk focus, this is represented by implementation of the National Strategy for the Prevention and Suppression of Terrorism by the respective authorities having anti–terrorism competences. No special focus is set by other authorities in their objectives and activities, which is a consequence of the poor assessment of the TF risks by the country and the level of displayed understanding.

143. Over the assessment period the objectives of the LEAs included goals to be achieved, such as “detection of suspicious financial transactions” and “search and identification of criminal assets”. As further described in the report, these goals were followed and achieved to a certain extent. Financial investigations are conducted regularly for all proceeds generating offences but mostly focused on direct proceeds of predicate offences. Little focus and achievements were demonstrated with respect to pursuing ML offence.

144. The objectives of the AMLO mostly derive from the findings of the NRA, the focus of the efforts being influenced by the priorities of the LEAs – the main users of the AMLO products. Monitoring trends and development of typologies usefully support the authorities’ and private sector’s AML/CFT efforts.

145. The objectives and activities of the CNB are informed by its own annual supervision plans. These are designed taking into consideration the EU Supranational risk assessment outcomes, the NRA and the sectoral risk assessment conducted by the CNB on an annual (for banks) or biennial (for other supervised sectors). Such an approach allows the CNB to better focus its activities, benefiting from a broader risk appreciation, which is especially important in terms of monitoring of the FIs that are part of a group structure. In addition, deeper understanding of the sectoral risks, which are not comprehensively reflected in the NRA, supports focused measures. The CNB, in particular, developed its new supervisory cycle around three main themes: providing services to non–resident customs (major typology); private banking (corruption – risk related to PEPs); and detection of the BO (tax evasion, drug trafficking and corruption – risks related to abuse of legal persons).

146. The objectives and activities of the Financial Inspectorate, similarly to the CNB, are informed by the own annual supervisory plans, which are designed on the basis of understanding of the risks in the supervised REs. This understanding is also based not only on the NRA findings but takes into consideration the risks common for the EU Member States and also ones that are specifically pertinent to the supervised population of entities. This is especially relevant for the MVTS and exchange offices sectors, which prominently featuring in criminal schemes.

147. The CFSSA acknowledged that their annual plans from 2015 to 2022 and annual work programme for 2019 to 2020 do not comprehensively reference AML/CFT matters. However, as of 1 January 2020, a unit responsible for AML/CFT matters within the CFSSA became operational, objectives and actions will better reflect on the ML/TF risks.

148. The TA, in the capacity of the gambling sector supervisor did not demonstrate having any distinct objectives set and actions taken. Supervision of AML/CFT systems of controls and compliance is only done as an additional function to the tax audits carried out by the TA.

### *2.2.5. National co–ordination and co–operation*

149. Competent authorities co–operate and co–ordinate on ML/TF issues in good spirit, but not comprehensively enough. There is a national level of co–ordination for implementation of the three strategic documents as analysed above and a high–level commitment. This, however, is not adequately present when it comes to combating ML/TF. Co–operation at an operational level is proven to be good. They do not do so to the necessary degree with regard to PF.

150. Co–operation and co–ordination on AML/CFT matters is entrusted to the IIWG – an expert working group composed of 11 competent authorities[114] in the field of AML/CFT, coordinated by the AMLO. This does not include policymakers – any senior officials, except for the representative of the SAO. In the AT opinion, this is a very core of the issue and explains the lack of a high policy level approach and support to effectively fight against ML and TF.

151. This issue is particularly apparent through analysis of the development and implementation of the 2016 and 2020 NRA Action Plans. Each of the agencies allocated with actions is left to elaborate and translate into practical terms how the action should be achieved. Additional work on co–ordination and co–operation seems to be more focused on operational activities rather than on strategically implementing the NRA Action Plans. The 2020 NRA Action Plan, in particular, does not allow for monitoring, measuring/assessing whether the actions that have been implemented and reporting on the goals/outcome achieved are supported by evidence and data. The summary of the agendas for the IIWG meetings did not include any assessment of the implementation of the Action Plans. Despite the requirement that implementation of the Action Plans should be discussed by the Government annually, there is only one report from 2018 that was presented, which still contained some actions to be implemented.

152. At the same time, the IIWG is an efficient platform for co–operation among the authorities at the operational level. The IIWG comprises two sub–groups: operational – the LEA and AMLO co–operation platform and supervisory sub–group – the supervisors and AMLO co–operation platform. These platforms help the experts to have not only formal co–operation but also swift

[114] The IIWG is comprised of the following competent authorities: Ministry of Justice and Administration, Security Intelligence Agency, State Attorney's Office, Ministry of the Interior, Ministry of Finance (AMLO, Financial Inspectorate, Tax Administration, Customs Administration), Ministry of Foreign and European Affairs, Croatian National Bank, and Croatian Financial Service Supervisory Agency.

and prompt bilateral communication, including informal and direct, at a person–to–person level. For this, Croatia should be commended.

153. The IIWG Supervisory Subgroup is established with the aim of strengthening coordination and exchange of experiences and best practices of the authorities in charge of monitoring the implementation of measures and actions to prevent ML/TF. Summaries of the agendas provided showed activity to providing common interpretations and guidance and preparation of the NRA. In particular, supervisors use this platform to discuss issues observed in understanding and implementing the AML/CFT requirements by REs and develop harmonised AML/CFT guidance to supervised entities. The CNB and Financial Inspectorate regularly use this mechanism to discuss entities in common (e.g., licensed by the CNB and supervised by the Financial Inspectorate) and misdemeanour proceedings. There was no reference to TA or the CFSSA using this mechanism for supervisory co–operation. There is little substantive supervisory interaction within this group regarding discussion of REs in terms of licensing, especially when rejecting or terminating a licence/permission of the RE or applying sanctions to members of the financial group under the control of various supervisors. While the authorities explained this to be done bilaterally, the AT is of the opinion that this subject should have more prominence in discussions within the sub–group. There is also room for further extension of the membership to the group, also engaging the SRBs that act as licensing/authorising bodies for DNFBPs. This would potentially have a positive impact, e.g., on strengthening their capacities and improving the market entry measures.

154. The IIWG Operational Subgroup was established to provide mutual feedback in specific cases related to ML/TF, to work on specific cases and coordinate actions. No minutes of these meetings were produced, but authorities advised that a number of meetings were held initiated by the SAO, and the MoI in the framework of co–operation on specific analytical cases. In addition, interactions also take place via informal communication.

155. The AT observed that while co–operation is established within the sub–groups, there is room for improvement in terms of interaction on operational matters between the sub–groups. The examples are participation of the supervisors in discussions of criminal cases where the supervised entities are involved. While the AMLO advised acting as an intermediary, the AT see the value in extending this to direct communication between the LEAs and licensing and supervisory authorities (including SRBs). This will be especially important for: (a) the licensing bodies, when providing authorisation and conducting ongoing monitoring of fitness and properness of the subjects (instances when authorised/licensed persons are suspected for criminal matters), and for suspension of such a person, where proportionate, until the criminal case is final; (b) the supervisory authorities, when monitoring the performance of REs (insights into the types of the REs utilised, the products abused, in the criminal offence) to inform their supervisory efforts and decisions; (c) for the LEAs, accessing the expertise of the supervisory authorities (knowledge of the business models of entities, mechanisms of abusing some financial and other products and services, etc.,) which otherwise would require considerable expense to acquire. A practical example to support the observation of the AT is that an SRB indicated that one of their members was facing criminal charges, and they only learned of this from the media and were subsequently contacted by this person directly; they were not informed of this by LEAs or the SAO, which effectively delayed the SRB response – cancellation of the issued license. (See also IO.3)

156. The Standing Group is the body responsible for implementation and monitoring of PF–related UN and EU sanctions regimes. Authorities confirmed that the Standing Group held

meetings for the purpose of discussing the amendments to the International Restrictive Measures Law (IRM Law) aimed at ensuring compliance of the legislation with the FATF Recommendations (the amendments came into force in June 2019). Representatives of various authorities took part in these meetings, some also represented in IIWG[115]. This co–operation, however, did not extend to exchange on operational matters.

157. Authorities also advised that the members of the Standing group are also the members of the Commission on the Prevention of WMD, which is responsible for the co–operation, information exchange and implementation of the activities related to the prevention of proliferation of WMD, as well as dual–use goods export control. There was no supporting information provided to verify the level and areas of interaction.

158. As also indicated in IO.10 and 11, there is an issue related to coordination between the MFEA, AMLO and the MoI on the receipt of the report on matches with the UN sanctions lists, which is a result of a low profile of the MFEA on this matter which leads to uncertainty among the REs about the appropriate addressee and the appropriate way of filing the reports.

### *2.2.6. Private sector's awareness of risks*

159. In order to inform the REs about the ML/TF risk environment of the country, both NRAs and Action Plans were published on the websites of the AMLO, CNB, CFSSA and the Financial Inspectorate.

160. The outcomes of the risk assessment were also communicated to the REs through the Annual AMLO Conferences, where all the supervisory authorities presented the ML/TF risks specific to their supervised sectors.

161. In addition, the CNB the Financial Inspectorate conducted training for the supervised REs where the participants were made aware of the ML/TF risks present in their respective sectors at an EU, national and sectorial levels. This training also included additional topics, such as interpretation of adopted subordinate legislation and the examples of good and bad practices in the implementation of all measures observed during on–site or off–site examinations. These were aimed at enhancing the response of the REs to detected ML/TF risks. The Financial Inspectorate also engaged the professional chambers.

162. Most of the REs demonstrated awareness of the results of the NRA. They have also acknowledged the usefulness of the outreach conducted by the supervisory authorities and the AMLO, noting that this contributed to their knowledge of the ML/TF risk environment in Croatia and developing of the respective response when conducting their activities.

163. The REs did not disagree with the assessment of risks in their sectors. Nevertheless, some of the groupings of sectors in the NRA assessment and assessment of controls in the DNFBP sectors were queried. The REs expressed the opinion that such an approach increases the ML/TF risk ratings assigned to their sectors, where if the sector had been assessed separately, the outcomes would have a more accurate reflection on the risks specific to their sector.

[115] Ministry of Foreign and European Affairs, AMLO, Financial Inspectorate, Customs Administration, Ministry of Justice, Ministry of Interior, State Attorney's Office, Security Intelligence Agency, Ministry of Defence, Ministry of Maritime Affairs, Transport and Infrastructure, CNB, CFSSA, Ministry of Economy, Entrepreneurship and Crafts.

### *Overall conclusions on IO.1*

164. Croatia did not demonstrate there is sufficient support at a policy–making level to combat ML/TF, which had an impact on the improvement of Croatia's ML/TF risk environment.

165. Croatia has made efforts to develop its understanding of ML/TF risks. The overall understanding of the ML risk is varied. The TF risk understanding did not prove to be sufficient across all authorities, with the CNB and the Financial Inspectorate demonstrating a comparably better understanding at a sectoral level. Overall, understanding of ML/TF risks was affected by several shortcomings related to identification and assessment of the ML/TF risks in Croatia. While there was overall awareness of various ML risks in the system, e.g., organised crime, use of cash cross–border risks, trade–based ML, risks related to VA and VASPs, deeper understanding was yet to be developed. Authorities did not demonstrate consideration of the TF risks that specifically could be emanating from OCG, migrant smuggling, remaining stocks of weapons and the financing of FTF family members. In certain instances, the magnitude of the impact of certain vulnerabilities on the risk environment of the country was not demonstrated to be understood, e.g., in relation to the gap in knowledge of ML and TF offences, systematic delays in judicial proceedings, shortage of human resources, issues related to maintaining criminal statistics, etc.

166. Croatia has developed three strategic documents in the area of suppression of corruption and prevention of TF, which, nevertheless, were not informed by the conclusions of Croatia about the ML/TF risks in the country. The two NRA Action Plans dealt with the ML/TF risks, but the substance and nature of the set actions with no overall strategic plan for the IIWG did not seem to set a policy. The objectives of the authorities are mostly led by their own observations and priorities, which while overall contributing to improvement of the risk environment in the country, nevertheless, are not sufficiently focused on and led by the detected national ML/TF risks.

167. The IIWG is an effective platform for operational co–operation and coordination on operational matters, for which Croatia should be commended.

168. **Croatia is rated as having a Moderate level of effectiveness for IO.1.**

# 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

## 3.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 6***

a) The competent authorities access a wide variety of sources of financial intelligence and other relevant information when conducting investigations. LEAs leverage financial intelligence mostly to develop evidence and trace criminal proceeds related to associated predicate offences. They rarely use these in the context of ML investigations and never for TF investigations (but were systematically used in TF pre–investigations led by LEAs).

b) LEAs co–operate with the AMLO to obtain relevant financial intelligence in the framework of their investigations. While most investigations are triggered by the AMLO disseminations (see IO.7), the ratio between these and launched investigations remains low. Limited feedback is provided by the LEAs to the AMLO to improve its operational analysis. Besides, the AMLO suffers from a significant shortage of human resources, which affects its performance.

c) The AMLO disseminates the results of its analysis to LEAs, but in some instances, these are addressed to the authorities with no law enforcement powers. While this is rarely done with respect to ML cases, the issue is systematic regarding TF, as cases are submitted to the SIA, but not to LEAs. This approach is further routed into the AMLO's procedure adopted in January 2021.

d) Once a case is identified, the competent authorities adequately and securely exchange information and financial intelligence. Nevertheless, the IT system has not yet been fully implemented to support electronic circulation of information among LEAs and the AMLO.

e) The AMLO conducts strategic analysis, however, it does not sufficiently reflect upon the higher risk areas identified in the NRA. Although the use of cash in ML–related scheme is a longstanding pattern, the AMLO does not appropriately use CTRs and cross–border reports to identify trends or patterns or trigger potential ML/TF cases.

f) STRs received, especially from banks and MVTS, contain relevant and accurate information, which assists the AMLO and LEAs when performing their duties.

g) Croatia introduced a new electronic reporting system for submitting STRs, which is used only by banks and the Croatian Post. Other REs submit STRs in white copies via post, which: (i) poses concerns as to the timing and confidentiality of reporting, and (ii) adds additional burden on the AMLO.

h) The lack of accuracy in certain statistics hinders the ability of the authorities to draw a full picture of the situation and actionable conclusions.

i) Considering the level of use of cash in the country, observed typologies, and the threshold for carrying out or receiving a payment in cash by legal persons in

Croatia which is HRK 75 000 (EUR 10 000), the current threshold for reporting cash transactions which is set at a level of HRK 200 000 (EUR 27 000) is deemed unreasonable.

***Immediate Outcome 7***

a) The legislation provides extensive powers to the LEA to identify and investigate ML. However, the ML is not prioritised as a national policy objective. Whilst various sources of information on eventual ML activity are on the LEAs' disposal (AMLO disseminations, in–coming MLA, evidence gathered through financial investigations, media reports), little evidence has been provided to the AT that these sources are extensively used to develop ML investigations/prosecutions, due to the main focus being on the predicate offences.

b) Judges, and to some extent prosecutors, demonstrated a limited understanding of some elements of the ML offence as envisaged by the relevant international standards (Vienna and Palermo Conventions). Namely: (i) opinion expressed in the Supreme Court jurisprudence suggested that depositing the proceeds of crime in the bank account of different natural persons is the only safe way to store money before its further usage; (ii) cumulative execution of all stages of ML (placement, layering and integration) is required; (iii) the high evidentiary thresholds for ML offence usually cause authorities to transfer the case to third countries where the predicate crime occurred.

c) Financial investigations are conducted as part of investigation of predicate offence. Whilst this is to be commended, these investigations and the evidence gathered throughout their course hardly triggered any ML related inquiry. Financial investigations mostly focus on the direct proceeds of predicate offences.

d) Predicate offences, some of which are rated as high ML threats (such as drug trafficking, corruption), are regularly investigated and prosecuted. However, these investigations and prosecutions rarely trigger further investigation/prosecution on laundering of proceeds gained by these offences and did not trigger any ML conviction. To some extent, this has also been acknowledged in the 2020 NRA.

e) Various reasons call for delays in criminal proceedings for ML and other complex predicate offences, which appear to be undue, have further diminished the effectiveness of the judicial system.

f) Whilst the legislation provides an adequate framework for pursuing different types of ML offences (self–laundering, autonomous and third–party ML), third party and autonomous ML investigations are not fully in line with Croatian ML risk. In addition, legal persons are rarely pursued in ML cases, despite the fact that the NRA notes a frequent misuse of "front" companies in such cases.

g) Criminal sanctions applied so far for ML offences are not sufficiently effective or dissuasive since they are minimal and appear not proportionate to the gravity of the crime and its associated risks. Suspended sentences are frequently

applied. The NRA pointed out the low level of sanctions for ML, but its action plan does not address this deficiency.

h) Croatia has some measures in cases where it is not possible to secure ML conviction, such as convicting for predicate offences and confiscation of proceeds, as well as non–conviction–based confiscation. NCBC appears not to be broadly used mainly due to its limited legal scope and, to some extent, due to the limited understanding of some practitioners on its application.

***Immediate Outcome 8***

a) Croatian authorities have legal powers to detect, restrain and confiscate instrumentalities, proceeds of crime and property of equivalent value. While there is no high policy document regarding confiscation, available legal instruments have been applied. However, the actions of the competent authorities in recent years demonstrate that confiscation is considered as a policy objective to some extent.

b) Croatia has confiscated significant proceeds of domestic predicate offences. There was no tangible result achieved with respect to confiscation for ML offences. Limited information was made available with regard to confiscation of proceeds of a foreign predicate offence. No TF–related confiscation has been achieved in Croatia so far.

c) The cases presented suggest that Croatia also confiscates instrumentalities and property of equivalent value. Sharing assets has been achieved to some extent even though the assessment team was not provided with exact numbers. Taking into consideration that the financial investigations are carried out as a part of the investigation of predicate offences, authorities do not keep statistics on those and cannot also provide results of the specific outcomes. This prevented the AT from having concrete insight into results achieved vis a vis committed predicate offence.

d) The difference between seized and confiscated assets is considerable. Assets may be temporarily seized for a maximum term of two years until the indictment is confirmed by the court. However, practice shows that undue delays in criminal proceedings of complex cases cause the release of the seized assets and create the risk of dissipation of assets. Effective recovery of confiscated assets is hardly achieved in those cases where provisional measures have not been applied.

e) The ability of the SAO to successfully conduct financial investigations and secure proceeds of crime are limited. This is caused by delays in setting up the Department for Investigation of Proceeds from Crime despite the SAO's legal framework providing the possibility to establish it.

f) In general terms, the Ministry of Physical Planning, Construction and State Assets (MPPCSA) properly manages a broad range of seized and confiscated assets, but regulatory limitations would prevent management of seized legal persons if the case occurs.

g) The CA monitors cross–border transportation of cash using various red flags or tactics during controls to determine the undeclared cash. Cross–border cash controls rarely triggered any further criminal investigations, and thus, there is no correlative conviction–based confiscation of illegal property (cash). Administrative sanctions applied for undeclared/falsely declared cash are *per se* low, but since this sanction cannot be followed anymore by confiscation of the transported cash, due to a change in the authorities understanding of application of legislation in place, it is considered to be not dissuasive.

h) Confiscation results are not always in line with the risk profile of the country described in both 2016 and 2020 NRAs. The majority of confiscated proceeds are associated with fraud which is rated as a medium ML threat. The amount of confiscated proceeds related to corruption, drug trafficking and tax evasion (posing high ML threat) is significant, but the volume is still not consistent with the identified ranking of types of threats. Confiscation related to ML offence is very limited.

***Recommended Actions***

***Immediate Outcome 6***

a) Croatia should ensure that the AMLO is provided with adequate human resources. The AMLO should fulfil its vacant positions with skilled professionals as a matter of urgency.

b) The AMLO should ensure that its cases are disseminated primarily to competent authorities with law enforcement powers, including by amending and further elaborating its dissemination procedures.

c) LEAs should provide regular feedback to the AMLO about: (i) the outcome and (ii) the quality of the financial intelligence received from the AMLO.

d) The AMLO should continue improving its operational analysis in line with the risk profile of the country. The AMLO should be more proactive in resorting to competent authorities to obtain relevant information.

e) The AMLO should improve its strategic analysis to identify emerging trends and typologies, focusing on the higher ML/TF risks. This should include leveraging on CTRs, cross–border cash declarations and other information.

f) The AMLO should: (i) provide more frequent, including, as required, a case–by–case feedback to REs on the outcomes and the quality of STRs; (ii) provide targeted guidance and training to REs on timely reporting of STRs; (iii) support the access by all REs to the new electronic system for filing STRs; (iv) consider adjusting the STR form to its needs.

g) Croatia should expedite the implementation of the new secure IT system to exchange information among LEAs and the AMLO.

h) Croatia should consider lowering the current threshold of cash transaction reporting and harmonising cash thresholds.

***Immediate Outcome 7***

a) Croatia should establish a national policy to prioritise identification, investigation and prosecution of ML cases in line with its risk profile.

b) Croatia should seek to ensure that judiciary and LEAs interpretations and understanding of the ML offence are aligned with the international standards, including by: (i) developing formal guidelines drawing on international and domestic requirements for ML offence and good practices for investigating and prosecuting ML offence; (ii) promoting evolving jurisprudence on ML cases in line with the current criminalisation of ML and international standards; and (iii) holding regular trainings.

c) Croatia should develop guidelines to assist LEAs in identifying and investigating ML offence which includes instructions on: (i) how financial investigations, incoming MLA/EIO requests, and information gathered through their own activities could trigger ML investigations; (ii) minimum evidence needed for investigation and prosecution of all types of ML offence, particularly in case of laundering foreign proceeds; (iii) tools and mechanisms to be used for gathering and threshold of evidence needed for investigation and prosecution of ML offence.

d) The LEAs should improve detection, investigation and prosecution of different types of ML, with a focus on the ML with foreign predicate offence and misuse of legal persons.

e) Croatia should carry out a comprehensive analysis of the reasons causing the undue delays in judicial proceedings of complex criminal cases and apply appropriate remedial measures. This could include, among others, considering legislative changes on conditions required to confirm indictment.

f) Croatia should revise criteria for imposing sanctions for ML offence to ensure the proportionality of these and consider also applying financial sanctions.

***Immediate Outcome 8***

a) Croatia should clearly establish confiscation of criminal proceeds, instrumentalities and property of equivalent value as a high–level policy objective. There should be specific actions aimed at tracing and securing direct/indirect proceeds, as well as foreign proceeds for confiscation purposes. The results achieved should be commensurate with the ML/TF risk of Croatia.

b) LEAs should develop clear guidelines for initiating and conducting parallel financial investigations aimed at the detection and tracing of domestic and foreign criminal assets, particularly in relation to ML and instrumentalities subject to confiscation.

c) Croatia should abolish legal deadlines for temporary seizure measures to prevent the release of seized funds before convictions are achieved and introduce periodic court controls (revision) of applied measures.

d) Authorities should ensure that adequate human resources are deployed in the Department for Investigation of Proceeds from Crime within the SAO, in order to make it operational.

e) Croatia should review the sanctioning regime related to the cross–border transportation of cash, considering the ECHR jurisprudence (v.g., Grifhorst v. France), to ensure that sanctions are proportionate, dissuasive and effective.

169. The relevant IOs considered and assessed in this chapter are IO.6–8. The Recommendations relevant for the assessment of effectiveness under this section are R R.1, R. 3, R.4 and R.29–32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

## 3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)

### *3.2.1. Use of financial intelligence and other information*

170. The competent authorities (the AMLO, the SAOs, the Police, the TA and CA) have direct and indirect access to a wide range of relevant information held by state authorities and the private sector. They actively communicate with each other to obtain necessary financial intelligence for their operational needs. The AMLO intelligence serves as a useful basis to trigger and support ongoing investigations and trace criminal proceeds. LEAs use it mostly to pursue investigations into predicate offences, and rarely into ML. This might be due to the LEAs' focus being on predicate crimes (see IO.7). In no instances did financial intelligence lead to TF investigations, though this was systematically considered when conducting pre–investigations by LEAs (see IO.9).

171. The LEAs (the Office for the Suppression of Corruption and Organised Crime (USKOK), other SAOs and the Police) have access to an extensive number of internal and external databases[116], which are updated on a regular basis. They have direct contact with the AMLO and REs to obtain financial intelligence and other types of information relevant for conducting investigations and tracing proceeds of crime. Except for the USKOK, which has powers to request bank account information directly, all LEAs shall require investigative judge orders to do so. In practice, these orders are obtained in a prompt and smooth manner.

172. The Independent Sector for Financial Investigations of the TA has access to a broad number of sources updated no later than every two weeks, including internal and external data. The CA has direct access to a set of competent authorities' databases[117]. The CA – when entrusted with investigative functions by the SAO – and the TA may request information from the AMLO.

173. The LEAs indicated making extensive use of this broad range of information sources to trigger both pre–investigations and investigations on ML and associated predicate offences.

[116] MoI data (on personal information, traffic documents, vehicle register) and the National Border Information system; Tax Administration, Customs Administration and AMLO data; Commercial Court Register; Municipal Court Land Registry Department; Unified Account Register; Land and Cadaster Register; Small Business Register (data on the small enterprise: name, address, owner, business operations); Register of Associations; Central Depository and Clearing Company; Croatian Register of Civil Aircraft (tail number, manufacturer, owner, address of the owner); Croatian Register of Shipping – CRS (basic information on the owner of the ship, port of registry, type of the ship etc. The database is searchable by the name of the ship, IMO number or CRS number); Financial Inspectorate, Croatian Financial Services Supervisory Agency and banks data; database of 'Poslovna Hrvatska' (Business Croatia).

[117] Tax Administration's data, MoI data and Passenger Name Record system.

Despite being granted access to the BO Register, they do not use it yet as it is very new and still being populated (see IO.5). In practice, they resort more actively to special evidence gathering actions when applicable.

174. The LEAs, in particular the Police, actively co–operate with the AMLO. When they identify an ML/TF suspicion, LEAs systematically send referrals to request additional information and/or support from the AMLO. In turn, the AMLO uses these referrals to open a case and conduct analysis of financial transactions. When it comes to ML–related referrals, the authorities suggest that LEAs, especially PNUSKOK, approach the AMLO primarily for information and analysis on cases linked to computer fraud, tax evasion, corruption and abuse of trust in business activities[118] (in decreasing order of volume), which correlates with Croatia's ML risk profile only in part. TF–related referrals were mainly sent to the AMLO by the Police, the SAOs and the SIA. They relate predominantly to financial transactions of foreign citizens with possible links to persons residing in territories controlled by the ISIL. They were used in the pre–investigative stage, but since they did not reveal elements of TF, none of the cases triggered an investigation (see IO.9).

175. The majority of the AMLO's ML spontaneous disseminations is submitted to the Police, the TA and the SAO. The vast majority of AMLO's TF disseminations is submitted to the SIA (see table under IO.9). The authorities suggest that most cases demonstrating the use of the AMLO's disseminations throughout the whole reporting period were related to economic crime and corruption (36%), tax evasion (26%), computer fraud (14%%) and organised crime (8%). This matches the type of referrals submitted by competent authorities to the AMLO, but not the pattern/quantity. In addition, it correlates to the NRA findings to some extent only: very few cases deal with illegal drug trafficking, which is one of the top three identified threats in the NRA.

**Box N°3.1: Criminal case based on AMLO dissemination**

In May 2020, a bank submitted an STR to the AMLO regarding a newly established Croatian company, which was receiving transactions from various Croatian companies and sending remittances abroad to several foreign companies. The AMLO carried out an analysis of all collected and available data, especially police data, and established that i) the owner of the Croatian company in question had committed 62 criminal offences in the field of economic crime in 2013–2014 and ii) the legal representative of one of the Croatian companies was linked to another Croatian company that was the subject of existing analytical processing by the AMLO, which also resulted in an operational analysis of transactions submitted to the TA and for information to the SAO in 2016. In June 2020, the AMLO disseminated the results of its operational analysis to PNUSKOK, the SAO and the TA. In July 2020, based on additional STRs from the same bank with the same pattern of transactions, the AMLO disseminated a 2nd operational analysis.

Consequently, the AMLO received a request from MUP PNUSKOK and was informed of an ongoing police investigation on the grounds of suspicion of committing offences of criminal association, abuse of trust in business operations, tax or customs evasion and ML committed by several natural persons using Croatian companies (including the new company) to issue invoices, transfer funds abroad and ultimately avoid paying VAT. The AMLO collected data from foreign FIUs and submitted a 3rd operational analysis of transactions to PNUSKOK in October 2020. In December, the USKOK informed the AMLO that one natural person purchased large quantities of dry–leaf tobacco abroad, intended to be sold in Croatia without paying excise duty. The AMLO

[118] Criminal Code, Art.246: illegal gain obtained from the property of others he/she has the duty to protect.

consequently requested information from foreign FIUs and, upon USKOK's request, gathered banking data.

On January 11, 2021, the Police and USKOK arrested several persons on suspicion of smuggling about 153 tons of tobacco as an organised group in Croatia and damaging the Croatian state budget for approx. HRK 122 mln. (EUR 16mln.) in excise duties. Searches of apartments, safe deposit boxes, houses, vehicles, business premises and warehouses in two Croatian cities resulted in the temporary seizure of 17 tons of tobacco, domestic and foreign paper money, two trucks and an expensive personal vehicle.

176. The LEAs expressed satisfaction with the financial intelligence provided by the AMLO. Nevertheless, the statistics provided below do not seem to confirm this statement (see table 3.1). Over the observed period, the AMLO disseminated a total of 1196 ML–related cases to LEAs, out of which LEAs used only 66 (about 5%) in their investigations. This low conversion rate might be the result of: (i) the high standard of proof set by jurisprudence; and (ii) the general lack of comprehensive understanding of the ML offence as it is envisaged by the relevant international standards by the judges and, to some extent, prosecutors (see IO.7).

**Table 3.1: AMLO's STR–based disseminations to LEAs and their development***

| Year | ML cases disseminated by the AMLO | ML cases used in investigations | ML investigations based on AMLO cases | TF cases disseminated by the AMLO | TF cases used investigations | TF investigations based on AMLO cases |
|---|---|---|---|---|---|---|
| **2015** | 205 | 10 | 4 | 4 | 0 | 0 |
| **2016** | 267 | 22 | 6 | 3 | 0 | 0 |
| **2017** | 208 | 9 | 3 | 6 | 0 | 0 |
| **2018** | 237 | 8 | 1 | 3 | 0 | 0 |
| **2019** | 137 | 8 | 2 | 7 | 0 | 0 |
| **2020** | 142 | 9 | 4 | 4 | 0 | 0 |
| **Total** | **1196** | **66** | **20** | **27** | 0 | 0 |

* The AT noticed significant discrepancies in the statistics provided by the Croatian authorities during the mutual evaluation period, which hinders its capacity to draw robust conclusions.

177. The Police received 498 ML cases during the observed period. As prescribed by the law, all of them were subject to a pre–investigation.

178. Throughout the reporting period, the number of ML pre–investigations by PNUSKOK has increased considerably (+67%, cf. table 3.2). This is due to an augmentation of the number of pre–investigations stemming from sources other than the AMLO (e.g., operational reports, statements, criminal reports, requests or orders by the SAO, requests of other organisational units of the Police, requests from INTERPOL, EUROPOL and other sources). This illustrates PNUSKOK's growing capacity to build in financial cases from its own sources, independently from the AMLO.

**Table 3.2: PNUSKOK pre–investigations on ML stemming from the AMLO and other sources**

| Year | AMLO | Other sources |
|---|---|---|
| **2015** | 81 | 135 |
| **2016** | 75 | 188 |
| **2017** | 85 | 136 |
| **2018** | 91 | 196 |
| **2019** | 77 | 268 |
| **2020** | 89 | 233 |
| **Total** | **498** | **1156** |

**Box N°3.2: ML investigation triggered by sources other than AMLO**

In 2016, based upon information obtained from its own intelligence, the Police conducted a criminal investigation against two Croatian nationals and one foreign national from a neighbouring country, who overtook a Croatian company that they intended to use for the transfer of criminal proceeds.

On 17.05.2016, a foreign company attempted to transfer the equivalent in HRK of 70,000 EUR to the above–mentioned Croatian company in an unauthorised manner via an unidentified computer system. However, the payment was not executed because the AMLO ordered the bank to temporarily cancel the transaction to the Croatian company's account, pursuant to the AMLTFL and based upon information provided by the Police and the bank.

On 18.05, the suspects arrived in a Croatian town intending to withdraw and share this money. The Police arrested them and temporarily seized their cell phones, business documentation, several bank cards, etc. On 20.05, as ordered by the competent County Court, searches of homes and other premises, including passenger cars, were performed. Objects potentially linked to the criminal offence were found, resulting in the regional branch of PNUSKOK filing a criminal report with the competent Municipal SAO against the above–mentioned natural persons and a legal entity for suspicion of ML.

On 17.08.2016, the competent SAO filed an indictment, and in December 2017, the competent Municipal Court rendered a final judgment of conviction for the criminal offences of ML for the above–mentioned natural persons and the legal entity.

179. The TA applies its own internal IT system to collect and monitor information on taxpayers. They perform their own inquiries based on the collected statistics and initiate tax procedures for determining breach of tax obligations and potential tax offences. The TA is also a recipient of the AMLO disseminations when they include suspicion of a tax offence. The authorities indicated that about 20% of AMLO's referrals are further investigated, which is indicative of the valuable analysis performed by the AMLO and the intense co–operation between both authorities. The TA also requests specific information on individuals or suspicious activities from the AMLO, both: (i) in cases opened based on the AMLO's submissions and (ii) in cases opened on its initiative. When the TA forms reasonable suspicion of a tax offence, they refer the case directly to the Police and the SAO. The TA demonstrated positive results using financial intelligence to develop not only tax–related but also ML cases, which subsequently led to investigation (see relevant case under IO.7). Given Croatia's exposure to tax evasion as one of the main predicate offences for ML, this practice represents a significant asset for the country.

180. The CA provides data on passenger movements, cash declarations, and cash seized to competent authorities through the Cash Declarations System. As indicated by the CA any ML/TF suspicion is reported to the AMLO: from 2015 to 2020, the CA sent 12 proposals for analysis, which the AMLO used to enrich its database and develop its cases. Analysis of these cases by the AMLO eventually did not confirm suspicions and trigger a dissemination to LEAs for further investigation. In turn, the AMLO disseminated two ML cases to the CA, regarding suspicion of ML–related excise fraud by foreigners that would potentially enter Croatia with undeclared cash. The CA took operational measures to detect the suspects of ML at the border control points. Nevertheless, this way of disseminating financial intelligence is questionable since such cases are primarily forwarded to the CA, thus before the SAO can entrust them with specific law enforcement powers.

181. It happens that in addition to the above–described instances, although rather rarely, the AMLO has disseminated ML cases also to some other competent authorities that do not have law enforcement powers. While it is not possible to estimate the size of the material impact of this practice, it still potentially represents missed opportunities for investigation.

182. With respect to TF cases, they are systematically exclusively disseminated to the SIA, which is not entrusted with law enforcement powers. While this illustrates tight co–operation between both agencies, not forwarding these cases to LEAs is a significant deficiency, especially since the SIA indicated that if it does not confirm the TF suspicion, it has no obligation to disseminate the case to LEAs. This is particularly appalling since there were no TF investigations over the assessed period.

183. The AMLO initiated a considerable number of suspensions and monitoring of transactions, both spontaneously and upon requests of LEAs (sometimes after they were submitted a case by the AMLO) or foreign FIUs. This demonstrates the capacity of competent authorities to identify and trace criminal proceeds, as illustrated in the case below.

**Box N°3.3: Suspension of a transaction initiated by the AMLO**

The AMLO started an analytical processing based on an STR submitted by a bank concerning large cash withdrawals (HRK 31 mln. (EUR 4.2 mln.)) from the personal account of KP, previously transferred from the account of his company E–P d.o.o. as loans or profit payments. On that basis, the AMLO received a proposal for analytical processing from the USKOK concerning suspicion of bribery and consequently performed checks on the accounts and safe deposit boxes of four natural persons. Based on this information and additional collected data from available databases, the AMLO established the suspicion of bribery.

As a result, the AMLO temporarily suspended EUR 652 897 and HRK 20 775 (EUR 2 770) of suspicious transactions on the account of one of the natural persons and submitted its operational analysis to USKOK. According to the information received from USKOK on 07.09.2020, inquiries carried out resulted in the identification of significant illicitly obtained property gain and the consequent pre–trial detention of the above–mentioned natural persons. Criminal proceedings are pending.

184. The AMLO actively resorts to its foreign counterparts (see IO.2) to gather financial intelligence when building its cases. Prior to disseminating information disclosed by foreign FIUs, the AMLO systematically asks for their approval, makes sure that the information is used for the purpose it was given and informs the foreign FIUs on the recipient of the dissemination.

**Table 3.3: AMLO disseminations to LEAs based on foreign FIUs information**

| Year | 2019 | | 2020 | |
|---|---|---|---|---|
| Offence | ML | TF | ML | TF |
| AMLO disseminations where foreign FIU spontaneous disclosures were used | 10 | 1 | 19 | 0 |
| AMLO disseminations where foreign FIU incoming requests were used | 20 | 1 | 19 | 0 |
| AMLO dissemination where requests to foreign FIUs were used | 70 | 1 | 46 | 0 |

### *3.2.2. STRs received and requested by competent authorities*

185. The AMLO is the central authority for receiving STRs, CTRs and cross–border declarations of cash and bearer negotiable instruments (BNIs).

*STRs*

186. In general, there are some concerns regarding the overall quality of STRs, particularly those that are filed by smaller REs. The authorities have taken efforts in recent years in this regard, increasing the communication with REs, updating guidelines and setting up conferences.

187. During the observed period, the AMLO has received 6 866 STRs, the majority dealing with ML and predicate offences, and 47 with TF. As the AMLO does not distinguish between ML and associated predicates when establishing their statistics, the exact share of these in the STRs could not be established.

**Table 3.4: STRs sent by banks, important sectors and others**

| Sectors | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | TOTAL |
|---|---|---|---|---|---|---|---|
| **Banks** | 670 | 776 | 616 | 634 | 704 | 2254 | **5654** |
| **MVTS** | 0 | 142 | 157 | 54 | 176 | 151 | **680** |
| **Croatian post** | 66 | 45 | 36 | 31 | 41 | 55 | **274** |
| **Currency exchange** | 6 | 1 | 2 | 17 | 2 | 4 | **32** |
| **Housing banks** | 5 | 14 | 0 | 6 | 6 | 8 | **39** |
| **Casinos** | 0 | 0 | 0 | 0 | 3 | 8 | **11** |
| **DPMS** | 0 | 1 | 0 | 0 | 0 | 0 | **1** |
| **VASPs** | 0 | 0 | 0 | 0 | 0 | 6 | **6** |
| **Real estate** | 0 | 0 | 0 | 1 | 0 | 0 | **1** |
| **Others** | 23 | 28 | 13 | 48 | 32 | 24 | **168** |
| **TOTAL** | **770** | **1007** | **824** | **791** | **964** | **2510** | **6866** |

188. The largest number of STRs come from banks followed by MVTS (including Croatian Post), which is consistent with the importance of these sectors. Reporting by other FIs and DNFBPs is low or non–existent, which is not always in line with the risk exposure of some sectors (see IO.4).

189. Some specific issues in the reporting prevent STRs from efficiently contributing to successful investigations of ML/TF cases. Indeed, the AMLO has acknowledged cases of non–reporting (ex. I–typology[119]), which upon identification are sanctioned as misdemeanours. In addition, in recent years, there have been some instances where smaller REs terminate business transactions/relationships in case of suspicion without filing an STR or filing it once the suspicious transaction has been carried out. These situations might represent missed opportunities for the AMLO to develop its analysis and are indicative of the need for additional targeted training on the steps to be taken once a suspicion arises.

190. Examples of STRs provided by the AMLO during the on–site were generally of good quality. Some were used in the AMLO disseminations and further pursued by LEAs. The STRs align with the risks identified within the NRA to a large extent and are relevant for detecting tax evasion and corruption, risks related to non–residents and use of fictitious legal persons and migrant trafficking. The authorities explained that REs have challenges in identifying suspicious transactions that would be related to drug trafficking patterns.

[119] I–typology – foreign citizens are opening bank accounts in Croatia in various banks in favour of which high value of suspicious funds are transferred from accounts opened in a foreign country's banks. The funds are subsequently withdrawn in cash or re–transferred to other natural or legal persons abroad.

**Box N°3.4: AMLO analysis based on an STR**

A bank submitted an STR concerning a wire transfer of 628,200 USD carried out on 04.10.2018, from the account of natural person Z (resident from country A) to the account of natural person Y (in country A) with the purpose of buying diamonds. The bank indicated that Z had opened a USD account in a bank branch in a Croatian town on 27.09.2018 and accounts in EUR and HRK the next day. In the information requested by the bank, he informed that he was an entrepreneur from country A, planning a large investment project in real estate in that same Croatian town, financed by his own company in country A. For this purpose, he created the company Z d.o.o., which also opened a bank account in the same bank on 27.09.2018, with no turnover. On 13.09, 52,500 EUR were transferred to the account of Z by a company based in country B, without a stated purpose. On 28.09, 1M USD were transferred to this same account by a company based in high–risk country C, with the purpose of transaction stating 'other escrow attorney'.

Since these are high–risk countries and Z did not inform the bank of such transactions, the bank requested documentation from Z regarding the remittances in question. Z indicated that he acted as an intermediary lawyer in a diamond purchase between the companies remitting funds and Y, the buyer. However, the contract he submitted to the bank did not mention the company in country C or Y. Instead, it mentioned company K as the seller and company G as the buyer.

According to publicly available sources, both companies were based in country D. Given the large amounts, several illogicalities (e.g., as a lawyer, the customer should have carried out the transaction through a giro account and not his current account; and the customer could have done this transaction through his account in his home country and did not need an account in Croatia), high–risk countries involved and discrepancies between the transactions and the CDD information, the bank decided to terminate the business relationship and check with the AMLO if the funds should be frozen before closing the account.

Following the STR, the AMLO performed further analytical processing of additional collected data, in particular data from foreign FIUs (namely of country A). The AMLO concluded on the suspicion that Z tried to conceal the real source of funds originating from fraud committed abroad. The AMLO issued an order for ongoing monitoring of the customer's financial operations and then issued orders for temporary suspension of suspicious transactions on the account of Z amounting to 370,000 USD and 130,000 EUR. The AMLO informed the competent local SAO on 22.10. The competent investigating judge confirmed the temporary suspension of transactions and prolonged it for two years. After ordering police inquiries, the local SAO transferred the prosecution against Z to the competent SAO in country A for the criminal offence of ML.

191. The AMLO highlighted their overall satisfaction with the quality of STRs provided, especially by banks, and to a lesser extent by MVTS and exchange offices. STRs from other FIs and DNFBPs, while to a varied extent, were considered as lacking in–depth analysis.

192. In order to improve the STR reporting, the AMLO takes various measures, including providing the REs with consultations via phone, periodically revising the Rulebook on STRs reporting and organising annual conferences. This ensures an interactive communication with REs, provides detailed guidance on information to be reflected in the STRs, and continuously updates the REs on emerging typologies and new red flags for identifying suspicious transactions. The usefulness of these measures was also confirmed by the REs, supervisors and SRBs. These efforts led to improving the STR submission in one of the important reporting sectors – MVTS.

193. The AMLO has paid specific attention to VASPs after the sector was designated as a RE, communicating their AML/CFT obligations. This focused approach is commendable, especially since VASPs are a new but emerging sector in Croatia, considerably rousing public interest.

194. In addition, in 2019, the AMLO adopted a new electronic reporting system for submitting STRs and CTRs, which aims at facilitating reporting practices. This system is used by banks and the Croatian Post. This, however, does not cover all the important reporting sectors (e.g., MVTS). The STRs submitted by other FIs and DNFBPs are sent via post, which poses the risk of timeliness and confidentiality. Upon receipt, they are typed in manually into the system, which, given the AMLO's limited resources, decreases its efficiency.

195. After receiving an STR, the AMLO regularly sends follow–up requests to the RE to get additional information, e.g., the turnover of a bank account (which is not accessible through the Unified Bank Account Register), the IP address used, or the authorised person on account of the customer. Although REs provide the additional information promptly (see para. below), given the AMLO's limited resources, this reflects on a potential need for expanding the STR template, especially where repetitive requests are observed.

196. With respect to access to information held with the REs upon request, the AMLO has indicated that requests are made smoothly to any RE, including to those who did not submit the initial STR, on a regular basis.

197. The authorities highlighted that when they request information from an RE, even though the legislative requirement is 15 days, in practice, they are provided with an answer within three days – or even less when urgent. During the reporting period, there were no instances of REs failing to provide the requested information on time. This demonstrates swift and fruitful communication with REs, even though, this legislative requirement does not seem to fit the necessity of prompt actions.

**Table 3.5: Number of AMLO requests sent to reporting sectors[120]**

| Reporting sectors | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | Total |
|---|---|---|---|---|---|---|---|
| **Banks** | 669 | 791 | 487 | 588 | 353 | 458 | 3346 |
| **Housing savings banks** | 0 | 8 | 2 | 3 | 2 | 0 | 15 |
| **Credit unions** | 1 | 0 | 0 | 1 | 0 | 0 | 2 |
| **Payment institutions** | 0 | 0 | 0 | 3 | 0 | 0 | 3 |
| **E–money institutions** | 0 | 0 | 2 | 1 | 0 | 0 | 3 |
| **Life insurance companies** | 0 | 0 | 0 | 0 | 0 | 2 | 2 |
| **Investment funds management companies** | 9 | 2 | 0 | 6 | 1 | 0 | 18 |
| **Pension companies managing voluntary pension funds** | 0 | 1 | 2 | 1 | 0 | 0 | 4 |
| **Leasing companies** | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| **Exchange offices** | 8 | 1 | 0 | 2 | 1 | 1 | 13 |
| **MVTS** | 2 | 3 | 5 | 1 | 0 | 12 | 23 |
| **Lawyers** | 0 | 1 | 0 | 1 | 0 | 0 | 2 |
| **Notaries public** | 3 | 0 | 2 | 3 | 0 | 0 | 8 |
| **Accountants** | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| **Real estate brokers** | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| **Games of chance** | 0 | 0 | 0 | 0 | 49 | 0 | 49 |
| **TOTAL** | **693** | **807** | **500** | **610** | **407** | **474** | **3491** |

[120] Reporting sectors, that are not displayed in this table, were not approached by the AMLO for additional information.

198. Despite the fact that the AMLO emphasises its daily informal communication with REs, the AT has concluded that the gaps in reporting are mostly due to the lack of sector–specific, case–by–case timely feedback on their reported suspicions. Indeed, feedback to the REs is often limited to the AMLO Annual Reports and conferences, which focus on the higher materiality reporting sectors. Although this corresponds to the NRA findings in terms of high ML/TF risk, the AMLO would benefit from expanding its outreach to sectors rated at medium ML/TF risk to adequately cover the reporting landscape of the country.

199. As indicated in the table below, the analysis of the use of STRs by the AMLO in its disseminations to competent authorities highlights a downward trend – from 52% in 2018 to 28.5% in 2020. It is observed that the decrease in the share of used STRs in disseminations is related to the fact, that recent supervisory attention paid to STR reporting led to a subsequent sharp increase in the number of STRs, but the quality of these did not follow the growth in numbers.

**Table 3.6: Share of STR received to the amount disseminated**

| Year | ML STRs received | TF STRs received (incl. UN TFS) | ML–related STRs used in disseminations | TF–related STRs used in dissemination (incl. UN TFS) | Total ML cases disseminated | Total TF cases disseminated (incl. UN TFS) |
|---|---|---|---|---|---|---|
| 2015 | 763 | 7 (1 TFS) | 314 | 4 | 205 | 4 |
| 2016 | 860 | 5 (1 TFS) | 353 | 4 (1 TFS) | 267 | 3 |
| 2017 | 663 | 4 (1 TFS) | 348 | 6 (1 TFS) | 208 | 6 |
| 2018 | 740 | 5 (1 TFS) | 386 | 3 | 237 | 3 |
| 2019 | 909 | 14 | 309 | 8 | 137 | 7 |
| 2020 | 2465 | 12 (1 TFS) | 703 | 4 | 142 | 4 |
| **Total** | **6400** | **47 (5 TFS)** | **2413** | **29 (2 TFS)** | **1196** | **27** |

200. As for TF reporting, the authorities and the private sector highlight that most TF–STRs stem from the banking and MVTS sectors, with the main reason for reporting being the geographical origin of the client. Such STRs generally involve remittance from conflict areas, where countries lack proper AML/CFT measures.

*CTRs*

201. In Croatia, the threshold for reporting cash transactions is set to HRK 200 000 (EUR 27 000). Since legal or natural persons carrying out a registered activity in Croatia shall not be allowed to receive or carry out a payment in cash equivalent to or above HRK 75 000 (EUR 10 000) (AMLTFL, Art.55), the AT interrogates the rationale for such a high cash reporting threshold. From 2015 to 2018, the annual number of reported CTRs has followed a constant increase. The authorities indicated that the downward trend observed in 2020 (see table under IO.4) is attributed to the COVID–19 pandemic.

202. The AMLO updated its Rulebook on reporting cash transactions in 2019. The authorities indicated that CTRs were correctly filled in by all REs. They contain information on the persons involved in the transactions, the transferred amount, the currency, the transaction account number and the location of the office where the transactions are conducted. CTRs are included in the AMLO database to inform their analysis.

*Cross–border reports*

203. The data from cash declaration forms are directly forwarded to the AMLO internal database by the CA. During 2015–2019, the CA filed 1 100 incoming and 491 outgoing cross–border reports, which serve as an additional source of information for the AMLO when examining a case. In addition, the CA sent 12 suspicious reports to the AMLO, which were related to cross–border transportation of cash (see case example under IO.8).

### *3.2.3. Operational needs supported by FIU analysis and dissemination*

204. The AMLO is autonomous and operationally independent in performing its duties, although being an organisational unit within the MoF. Since 2017, the AMLO budget has been explicitly indicated as a separate Article under the MoF budget, providing distinct financial and human resources, IT and technical equipment.

205. Within the whole period under review, the AMLO has suffered from a shortage of human resources that has affected its ability to fully perform its duties. This has been recognised by both NRAs and has been included in both Action plans. Despite the recent efforts of the AMLO management (two staff members hired in 2021), there have been no significant change in the situation over the observed period. As of 2020, there are nine employees in the AMLO's service for financial analysis (and three vacant positions) and four employees in the service for prevention and supervision of REs (and 7 vacant positions).

**Table 3.7: Human resources of the AMLO**

| Year | Systematised work positions | Number of employees | % of employees |
|---|---|---|---|
| 2015 | 34 | 22 | 64,70% |
| 2016 | 34 | 21 | 61,76% |
| 2017 | 37 | 21 | 56,76% |
| 2018 | 38 | 21 | 55,26% |
| 2019 | 38 | 19 | 50,00% |
| 2020 | 37 | 20 | 54,05% |

*Operational analysis*

206. The AMLO performs an operational analysis of STR through the Service for Financial Intelligence Analytics. Internal written procedures describe the process of carrying out the relevant steps of the analysis, guiding the efforts of analysts when needed.

207. The analytical staff of the AMLO, although limited, is experienced and well–trained. Until 2019, the average number of STRs analysed per analyst amounted to one per week. Yet, after the increase in reporting in 2020, each analyst has to deal with one STR per day and a half, making it hardly possible to meet the necessary procedural requirements on time.

208. When conducting operational analysis, the AMLO routinely utilises its powers to access a number of databases kept by competent authorities. The AMLO stated to make active use of the newly set–up BO Register, noting this was used in all analysed cases. The AMLO has a dynamic internal database that encompasses a broad range of information from private and public sectors, including foreign sources.

209. The information contained in requests from LEAs are included in the newly updated AMLO IT system, which allows for a swift mapping of cases. Often, these requests: (i) help to establish a link with an ongoing investigation, (ii) facilitate decisions on dissemination and (iii) enrich the AMLO database with practical cases. Such practice presents an asset and demonstrates proper

use of LEAs' information for the AMLO analytical purposes. The IT system, jointly with the wide range of information accessed by the AMLO, contributes to the quality of the AMLO analysis.

210. Upon receipt of the STR, the analyst conducts a qualitative check to ensure that all required fields are completed and flags the potential need for additional information or clarifications. At this stage, the analyst checks for the client's BO, status as PEP, the purpose and the amount of the transaction to determine whether prompt actions such as suspension of funds are needed. This is followed by an intelligence check, i.e., searches for links of natural and legal persons subject to reporting in the AMLO IT system and other relevant databases.

**Box N°3.5: STR–based operational analysis further investigated by LEAs**

The AMLO started an operational analysis based on a bank STR relating to wire transfers from Croatian companies to the business account of company A d.o.o. with the purpose of "*loans, material costs, purchase of raw materials*". These funds were then withdrawn in cash by natural person OK, owner and proxy of company A. There were no other activities on the account. However, the AMLO established that between December 2016 and February 2017, company A received a total of 1,188,758.07HRK from other Croatian companies on business accounts opened in four different banks, which were ultimately withdrawn in cash.

The AMLO identified that OK had been the subject of a previous analytical processing where they determined that in 2015–2016, he was owner and director of another Croatian company being part of a network of companies that transferred funds among each other, which were ultimately withdrawn in cash. The AMLO established the suspicion of tax evasion and concealment of the real source of funds and consequently disseminated its findings to TA in October 2018.

In connection with AMLO's dissemination and subsequently submitted additional data from April, May and June 2020, the USKOK informed the AMLO of the decision to investigate natural persons TP and OK based on suspicion of ML, and against other eight associates. The criminal charges in this case were filed primarily by the TA and PNUSKOK in May 2020, based on the results of special evidentiary actions ordered by the investigative judge and conducted in May 2019.

The authorities established that in 2017–2019, TP and OK, as business managers of numerous legal entities registered in different areas of Croatia, connected several persons with the aim of obtaining undue property gain by illegally reducing VAT on various products. Part of this gain was integrated into the financial system through wire transfers amounting to HRK 6 031 963, stating that these transactions were loans and contractual payments in favour of related legal entities B d.o.o. and C d.o.o. Ultimately, the funds were intended to acquire real estate.

211. STRs are prioritised as 'high', 'medium', or 'low' according to relevant weighted criteria[121], which do not consider the areas of higher risk as reflected in the NRA. Due to the limited timeframes required to secure the postponement of a transaction[122], the highest priority is given to analysis of STRs requiring potential suspension, then to STRs featuring natural persons already involved in an AMLO case. 'Low–priority' STRs typically include low amounts or absence of formal establishment of the source of funds by the RE.

[121] I.e., whether the client is a PEP, and/or the money was to be drawn from the account within 30 days of creating account, the amount – over HRK 3M, more than 5 transactions within 30 days, customer is involved with AMLO case, customer is investigated, prosecuted or convicted for ML/TF. Furthermore, the AMLO prioritises foreign FIU requests, where urgent action is required due to the temporary suspension of suspicious transactions, and/or the domestic State body requests urgency.

[122] 120 hours from the moment of issuing the order to the RE (AMLTFL, Art.117(2)2)

212. The authorities indicated that high–priority STRs result in immediate analysis, while medium and low–priority ones are added to a new case and will be analysed at a later stage. However, there are no specific timeframes for carrying out the analysis per category. The AMLO indicated that although the timing may vary depending on the nature and complexity of the case, timely execution is always ensured. There is no clear process to decide which analyst will work on which case, but the AMLO specified that the most complex ones are given to the most experienced analysts.

213. When it comes to requests received from competent authorities or foreign FIUs, the AMLO systematically gives them priority when they are indicated as 'urgent'. However, there is no formal prioritisation of these requests in the IT system.

214. Over the reporting period, the AMLO received 47 TF–STRs. Out of these 47 STRs, five were TFS–related and were filed by REs because of a match (false positive) with the UN TFS lists. The AMLO disclosed two out of these five STRs. When receiving the TFS–related STR, the AMLO performs checks in its databases but does not further explore except for requesting further information from other relevant sources.

215. When analysing the STRs on TF suspicion, the AMLO demonstrated checks the natural and legal persons involved against the available databases, investigates their network and transactions and requests additional information from REs when relevant (see case under IO.9). When analysing such STRs, the AMLO leverages international co–operation to obtain further data. Nevertheless, when it comes to domestic authorities, the AMLO does not resort to the SIA to get additional intelligence to build its case. Rather, it forwards it straight to the SIA.

216. A similar approach of the AMLO is also observed when dealing with ML and related predicate offences. The AMLO uses a broad range of accessible data, information from foreign FIUs (see IO.2) and REs, but it does not proactively request additional information and intelligence from competent authorities to further develop its cases.

217. The AMLO is making appropriate and efficient use of the suspension measure. After suspending suspicious transactions, the AMLO substantiates it to the competent SAO, who then obtains a Court order for further suspension of the transaction lasting up to two years (see also IO.8). In practice, it is provided smoothly. Within the reporting period, there were no cases of false/ungrounded initiation of this procedure. Neither were there detected cases where the suspension of a transaction would have hindered an ongoing investigation by LEAs. However, the AMLO has indicated a few cases of reporting once the transaction is carried out, which can represent potential missed freezing opportunities.

218. There is no linearity regarding suspension of suspicious transactions (see table 3.8). The authorities were not able to explain the year–to–year fluctuation.

**Table 3.8: AMLO orders for temporary suspension of transactions**

| Year | No of issued orders initiated by: | | | | Total | Amount (EUR) |
|---|---|---|---|---|---|---|
| | AMLO | SAOs | Police | CA | | |
| **2015** | 47 | 5 | 2 | 0 | 54 | 10 212 460 |
| **2016** | 69 | 7 | 2 | 5 | 83 | 8 460 200 |
| **2017** | 16 | 25 | 0 | 0 | 41 | 1 428 680 |
| **2018** | 75 | 0 | 5 | 0 | 80 | 10 500 000 |
| **2019** | 19 | 14 | 2 | 0 | 35 | 4 106 660 |
| **2020** | 43 | 2 | 1 | 0 | 46 | 4 515 762 |
| **TOTAL** | **269** | **53** | **12** | **5** | **339** | **42 041 162** |

**Box N°3.6: Suspension of transaction and autonomous ML indictment**

The AMLO initiated this case based on an STR. DM (non–resident), director of company AT located in country A, had issued payment orders amounting to EUR 3 285 354 in favour of company Z Ltd., located in Croatia. Based on a loan agreement, the owner of the company Z (ZK, Croatian resident) then transferred EUR 1 950 000 to DM's personal account in country A, and the rest of the funds to accounts of ZK, his family members and company Z.

After receiving intelligence that there is an ongoing criminal procedure against company AT in country A, the AMLO issued an order for temporary suspension of execution of transaction amounting to EUR 516 007 and disseminated the case to the competent SAO. The Municipal Court in Osijek confirmed indictment against natural person ZK and legal entity Z for the criminal offence of ML. To conceal and disguise the true nature and location of proceeds of crime, it was confirmed that ZK had incorporated company Z, which issued 11 invoices to the company AT for brokerage services that were not provided.

219. In addition, the AMLO can apply orders for ongoing monitoring for maximum six months[123] to prevent certain funds from being withdrawn or remitted through non–cash remittances without the AMLO being informed about it by the RE. Monitoring orders are mostly used on accounts where suspicious transactions have been previously detected or on inactive accounts, which might be used for criminal purposes in the future. The AMLO indicated that in 90% of the cases, the funds ended up being frozen, which confirms the usefulness of this measure to trace proceeds of crime.

**Table 3.9: Orders for continuous monitoring of customers' financial operations**

| Year | Monitoring orders |
|---|---|
| 2015 | 64 |
| 2016 | 70 |
| 2017 | 3 |
| 2018 | 97 |
| 2019 | 18 |
| 2020 | 49 |
| **TOTAL** | **326** |

*Strategic analysis*

220. The Service for Strategic Analysis and Information System of the AMLO carries out strategic analysis of the data collected from the REs, the competent authorities and the foreign FIUs. This input contributes to establishing the most common typologies and trends in ML included in several Annual Reports[124]. These reports are distributed to competent authorities and made available online to REs, which highlights their usefulness.

221. These strategic products are a valuable basis to enrich LEAs' knowledge and target their investigations. Nevertheless, limited strategic analysis is conducted on any higher risk areas, including use of cash, corruption, drug trafficking, OCG or potential TF. Only a small fracture of NPO transactions has been analysed without drawing strategic conclusions.

[123] AMLTFL, Art.119: orders for ongoing monitoring of a customer's financial operations may last for maximum three months, and in justified cases the duration of the order may be extended each time by another month (the execution of the order may last a maximum of six months).

[124] AMLO Annual reports include strategic analysis on suspicious transactions, cash transactions, ML/TF typologies and trends and a dedicated report for the REs on aggregated feedback of the submitted STRs.

222. Acknowledging that the use of cash in ML–related schemes is identified as a longstanding pattern in Croatia, the AMLO analysis of CTRs or cross–border reports to contribute to strategic products is not comprehensive enough. In addition, this prevents the AMLO from detecting potential ML suspicions or schemes, which is aggravated by the fact that REs do not consider 'just–below–the–threshold' cash transactions in their reporting.

*Dissemination*

223. The AMLO disseminates data and information to the relevant competent authorities both upon request and spontaneously, based on sufficient grounds to suspect that ML, associated predicate offence or TF has been committed. There is an established practice for deciding to which authority the AMLO discloses its case: upon the proposal of the case analyst and some unofficial communication with the interested authorities, the Director of the AMLO, in consultation with his Deputy and the Head of Service, decides on the recipient of the case by taking into account: (i) the finding of the case, and (ii) the prerogatives of the relevant domestic or foreign authority.

224. In practice, the AMLO disseminates cases mainly to the MoI (around 31%, mainly PNUSKOK), TA (26%), SAOs (19%), and the USKOK (4%). The share of disseminations among the authorities remained stable through the whole period. It has come to the attention of the AT that in some instances, the AMLO disseminates ML cases to competent authorities without law enforcement powers. This is somehow mitigated by the fact that SAO is in copy of all the disseminations and is thus able to redirect the case if needed. This is, however, not the case with TF disseminations, which are systematically exclusively directed to the SIA (see 6.1), which has no law enforcement powers. In the AT's view, such practice illustrates a wrong decision–making of the AMLO, which is considered as a major deficiency since it does not adequately support the operational needs of investigative bodies.

225. LEAs provide little feedback to the AMLO on the quality and the use of their disseminations. Most of it comes from the TA. The AMLO also receives periodic statistics on the criminal investigations from the SAO, which cannot be considered as a feedback on the disseminations submitted because it lacks input on the quality and relevance of the analysis conducted by the AMLO. The Police send feedback to the AMLO in the form of an annual report and in isolated instances, on specific cases. In addition, the MoI informs the AMLO on the number of disseminations, which did not result in ML investigations, but were used in inquires resulting in investigations for abuse of trust, tax evasion, etc.

226. Overall, the lack of detailed, case–by–case feedback from the LEAs prevents the AMLO from: (i) assessing the usefulness of its disseminations, and (ii) the adequacy of the recipients of its disseminations. Such feedback would allow the AMLO to appropriately align its efforts with the priorities of the LEAs in line with the risk profile of the country and enhance coordination in the AML/CFT efforts among competent authorities.

### *3.2.4. Co–operation and exchange of information/financial intelligence*

227. There are no legislative or other barriers hindering the proper co–operation or exchange of information between the AMLO and other competent authorities. No cases of refusal of co–operation nor delays were reported to the AT. In practice, competent authorities respond to requests from the AMLO within two weeks. Although this has never led to serious delays, the AMLO would benefit from prompter responses from the authorities to build its cases.

228. The IIWG, which gathers representants of the eleven AML/CFT public stakeholders in Croatia, constitutes an adequate forum to share information and good practices among competent authorities and foster co–operation. Several meetings were held initiated by the SAO and the MoI in the framework of co–operation on specific analytical cases.

229. The AMLO, the PNUSKOK, the USKOK and competent SAOs, the TA, the CA and the SIA daily exchange information on relevant cases through secure means. The AMLO excessively relies on informal channels of communication such as phone calls with REs, which ensures prompt exchange of information and allows to take quick actions – in particular, this is systematically done prior to initiating a formal postponement order. Data confidentiality is always ensured. Rules in place for access to the databases, premises and documents are appropriately applied. Disseminations are conducted in hardcopies, however, the authorities indicated that there was never a case of leaking or losing information thus far, and the AT did not come across such information. In addition, Croatia is developing an IT tool that will securely connect all AML/CFT stakeholders. The AMLO has taken the lead by implementing and developing this system already.

230. The AMLO also regularly communicates with the supervisors (CNB, CFSSA, Financial Inspectorate and TA) in the framework of AML/CFT supervision of REs. They submit cases to the AMLO whenever they come across suspicions of ML, associated predicate offences or TF in the course of their supervisory duties. In turn, if the AMLO flags a situation of misreporting, it has the capacity to ask the supervisors for targeted supervision of a specific entity. In addition, the AMLO coordinates its efforts together with the supervisors towards providing training and guidance to REs, especially during annual conferences.

### *Overall conclusions on IO.6*

231. LEAs have broad and smooth access to financial intelligence and other relevant information, and actively communicate with each other and with the AMLO during the course of their investigations in a secure manner. Despite its apparent lack of human resources, the AMLO has shown cases of valuable operational analysis based on the inputs from REs and other sources. The STRs from the most important sectors are mostly of good quality, triggering the AMLO disclosures. These represent the strengths of the Croatian system regarding the use of financial intelligence and other relevant information in conducting operational activities and investigations.

232. Nevertheless, LEAs use this information primarily for investigation of predicate offences, to a lesser extent ML. While most criminal investigations are launched by LEAs on the basis of the AMLO disseminations, the share of these remains modest. As for TF, financial intelligence and other information are used for pre–investigations only. There are some issues with the AMLO disseminations to LEAs in respect to ML cases, which are systemic when it comes to TF cases, as they are submitted to the SIA but not to LEAs. Lack of feedback from LEAs to the AMLO hinders the coordinated response of the authorities to the main ML/TF risks. At the same time, limited feedback and guidance of AMLO towards REs limits the adequate response of the private sector to suspicious behaviours.

233. Overall, the system requires major improvements to ensure effective use of financial and other information for pursuing ML, associated predicate offences and TF investigations.

234. **Croatia has achieved a Moderate level of effectiveness for IO6.**

## 3.3. Immediate Outcome 7 (ML investigation and prosecution)

235. In Croatia, multiple competent authorities with different powers are involved in detection of ML such as the AMLO, the custom and TA (Sector for financial investigations), the Police (PNUSKOK), whereas the SAO supervises the procedure and further leads criminal investigations ex officio. A previous inquiry stage is usually conducted to ascertain the existence of sufficient grounds to launch a criminal investigation. Once the SAO launches a criminal investigation, the police execute its orders, and, if required, officers of CA and TA are appointed for investigative purposes.

### *3.3.1. ML identification and investigation*

236. Croatia has extensive legal powers enabling identification and investigation of ML. However, achieved results show that ML offence related to the predicate offences posing a high level threat are identified and investigated to an insignificant level. A number of authorities can be involved in identification of ML but mainly focus on the investigation of the predicate offence rather than on the ML.

237. The authorities advised that potential ML cases would be identified from various sources such as:

-following the dissemination made by the AMLO;

-during the course of investigation of a predicate crime;

-as a result of financial investigation;

-based on the information provided by the foreign counterparts, including MLA requests.

238. According to statistics[125], ML cases are mainly triggered by the AMLO dissemination.

**Table 3.10: Total number of ML investigations, prosecutions and convictions**

| | **Investigations** | | | **Prosecutions** | | | **Convictions (first instance)** | | | **Convictions (final)** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Cases | | NP[126] (LP)[127] | Cases | | NP (LP) | Cases | | NP (LP) | Cases | | NP (LP) |
| | AMLO | other sources | | AMLO | other sources | | AMLO | other sources | | AMLO | other sources | |
| **2015** | 4 | 2 | 10 (–) | 4 | 3 | 16 (–) | NA | – | – (–) | 1 | 2 | 4 (–) |
| **2016** | 6 | 6 | 49 (1) | 7 | 6 | 33 (4) | NA | 1 | 2 (–) | 2 | 2 | 6 (1) |
| **2017** | 3 | 2 | 10 (1) | 4 | 5 | 17 (1) | NA | 2 | 6 (–) | 3 | 3 | 5 (–) |
| **2018** | 1 | 1 | 10 (–) | 3 | 2 | 16 (1) | NA | – | – (–) | 3 | – | 6 (–) |
| **2019** | 2 | 3 | 18 (2) | 2 | 1 | 21 (1) | NA | 1 | 1 (–) | 2 | 1 | 4 (–) |
| **2020** | 4 | 4 | 22(2) | 1 | 3 | 5(2) | NA | 2 | 5 (–) | 1 | – | 1(–) |

125 Statistics provided by Croatian authorities are often not consistent with data previously reflected in the MEQ or the NRA.
126 Natural person (NP)
127 Legal person (LP)

239. A low number of the AMLO's disclosures triggered ML investigations/prosecutions (see also IO.6). This can be explained because of the fact that the standard of proof set by jurisprudence is perceived as being considerably high. Furthermore, there is a general lack of comprehensive understanding of the ML offence as it is envisaged by the relevant international standards (Vienna and Palermo Conventions) by the judges and to some extent by prosecutors, which has a cascading effect on the identification of ML offences by the Police and other LEAs.

240. Judges and several prosecutors confirmed that the purposive element of concealment is required, in practice, by Courts with regard to all ML conducts (including the conducts acquisition, possession and usage of proceeds). In the view of the assessment team, this has a cascading effect on the low number of identification/investigations of ML cases. Furthermore, jurisprudence shows that the extent to which the ML offence is understood in Croatia is inconsistent with the incrimination in the CC, as well as requirements of the international standards. Namely, it is a common understanding that depositing the proceeds of crime in the bank account of different natural persons is the only safe way to store money before its further usage. In addition, it seems that the cumulative execution of all stages of ML (placement, layering and integration) is required by the jurisprudence of the Supreme Court[128].

**Box N°3.7: Supreme Court Judgement[129]**

Two persons obtained HRK 8.7 mln.. (EUR 1.1 mln.) from a criminal offence and deposited this money in more than 10 bank accounts owned by third persons (relatives acting as strawmen) and finally withdrew this money. The first instance court found them guilty of predicate crime (economic crime), as well as money laundering. However, Supreme Court decided that in this specific case, there is no ML offence and stated the following: "*the mere fact that the defendants, after illegally acquiring money, deposited the same money in their accounts (as well as the accounts of their close relatives) opened with various banks, and which money was then withdrawn from those accounts, does not constitute action in a banking business that conceals the real source of the money. Money deposited in a bank account would represent only the first of the three stages of the money laundering process, i.e., only the physical entry of cash of criminal origin into the banking system, and the stage of financial transaction concealing the origin of money and the stage of integration which is "dirty" money became legal income. Therefore, depositing money in a bank account and then withdrawing it is only the use of the bank as a convenient, safe place to store money before its further use and therefore does not constitute a feature of the offence*".

241. Although authorities argued that the opinion expressed in the Supreme Court judgements are not mandatory for the other courts and prosecutors' offices, since it does not represent a compulsory legal opinion, judges and several prosecutors confirmed that they agree with its findings and conclusions. Some prosecutors also brought the arguments that after these judgements, there have been amendments of the incrimination of ML offence in CC which can influence future jurisprudence to be different. However, this was not possible to confirm since no conviction was brought so far to oppose existing Supreme Court judgements. In addition, the 2020 NRA still considers Supreme Court judgements as an impediment to effective investigation and prosecution of ML offence and does not indicate that they have been superseded by new legislation.

128 Supreme Court Judgements I Kz 625/13–6 (08.05.2015) and I Kz 560/16–4 (08.09.2016)
129 Supreme Court Judgement I Kz 625/13–6 (28.05.2015).

242. The high standard of proof set by jurisprudence and lack of comprehensive understanding of ML offence also have an impact on the low number of ML investigations triggered by the performance of LEAs (police, custom, TA). Despite the fact that the exact number of ML investigations triggered by different LEAs has not been presented to the assessment team, this conclusion is drowned from the general statistics, as well as from the contributions provided by the authorities.

243. **Police** identify and investigate some complex, transnational organised crime cases, including drug trafficking–related cases. Several complex case examples were presented, however, a limited number of cases triggered ML prosecutions. This is mainly caused by a high level of the evidentiary threshold set for ML offence, as well as by the lack of a comprehensive understanding of the nature of this offence. Usually, when the predicate crime is being committed in a foreign jurisdiction, the case is transferred to that country without further investigation on the national level to determine ML offence. While authorities stated that in most of those cases, they did not timely receive assistance from foreign countries in order to pursue ML investigation and prosecution, this argument was not supported by the number of MLA and EIO requests sent for ML offence (see IO.2), as well as by presented cases.

**Box N°3.11: Complex organised crime case "La Familia"**

In 2017 Croatian law enforcement authorities initiated inquires on an organised criminal group smuggling cocaine from South America to Europe through Croatia. Croatian authorities co–operated with counterparts from several countries (including Hong Kong) with the support of EUROPOL and EUROJUST. Members of the organised criminal group smuggled cocaine from South America to Europe and Asia and registered a company in Croatia (using false identity), opened several bank accounts, bought aircraft for smuggling cocaine, made fake commercial flights etc. The group was monitored during 2018 and 2019, and several cocaine smuggling operations were recorded. Police seized over a ton of cocaine, particularly 600 kg in Switzerland and over 400 kg in Hong Kong. In addition, in October 2019, at the Croatian border, a vehicle was searched, and around EUR 1 mln. were found. As a result of this operation, 15 persons have been arrested in several different countries, and most of them have been extradited to Croatia to be prosecuted. The Croatian authorities prosecuted them for organised crime and drug trafficking, and for one person, they transferred proceeding to a neighbouring country for ML offence.

244. The TA systematically analyses information of its databases, documents, and accountability of taxpayers and requests information from the AMLO. If further actions are needed, such as special investigative techniques, the case is referred to the SAO. In this context, 39 criminal reports were filed by the TA–Independent Sector for Financial Investigation from 2015–2020. The total amount of money related to these reports is HRK 2 086 mln (EUR 274 mln.), including only a single but significant ML–related case of HRK 631 mln. (EUR 80 mln.), which finally was not prosecuted for ML, but only for tax offence. Furthermore, tax authorities indicated that only in 2020 have they filed two criminal reports for ML offence and the total amount of laundered money is around HRK 22 mln. (EUR 3 mln.). However, no additional information has been provided to the assessment team about further investigation and prosecution for ML offence. In some of the ML cases triggered by the TA (in co–operation with the AMLO), ML indictment has been brought, but those are relatively simple cases (particularly compared with the Gold case).

**Box N°3.12: Complex organised crime case "Gold"**

A largescale tax evasion case involved 15 natural persons. They were detected and investigated by the Independent Sector for Financial Investigation in coordination with USKOK and PNUSKOK. Special investigative techniques were used but mainly oriented to establish the predicate offence of tax crime. This case was triggered by a financial investigation.

According to the indictment, between 2014 and 2016, the defendants bought gold and other precious metals on the black market and sold them to third persons, namely to Italian companies. This sale was executed through three Croatian companies managed and owned by members of the criminal group. These companies issued invoices (over HKR 640 mln.) to Italian companies for the delivery of the referred items. Further, unjustified payments were made to natural and legal persons for goods that were not actually delivered. At the same time, they ordered the posting of a part of the fake invoices and contracts of these natural and legal persons, including fake invoices of alleged suppliers.

After the execution of planned transactions (i.e., payments of funds into accounts of natural and legal persons based on false documentation), the money coming from these actions was withdrawn in cash by some members of the group after other members converted it in banks and exchange offices into euros and other currencies, in order to give this money to the leaders of the criminal group.

According to the information provided by some Croatian authorities, the standard of proof of the subjective element of ML impeded the prosecution of this case for ML, but it was prosecuted for a predicate offence.

245. The CA demonstrated some positive practices by regularly conducting different types of actions to detect smuggling and drug trafficking at the borders, identifying Croatia as a transit point. The CA confirmed that criminal reports are also disseminated to the SAO and police, especially in relation to smuggling of tobacco. However, it seems that there has been a lack of understanding of what actions need to be undertaken in order to detect ML offence. Therefore, according to the information provided, no ML–related case has ever been pursued.

**Box N°3.13: Cash–related control at the border**

A traveller coming from the route Vietnam–UAE–Belgrade–Zagreb on 28 August, 2017 was controlled by the CA in the "*green line*" (i.e., nothing to declare) of the airport of Zagreb. CA officers searched his luggage and found USD 350 000. The suspected person stated that the origin of the money was from a bank in Dubai and represented his income. His intention was to use the money to buy personal vehicles/real estate in Croatia.

This information was sent to the Financial Inspectorate for sanctioning purposes. However, based on the information received during the misdemeanour proceeding, FI sent a request to the AMLO. The operational analysis was undertaken, and based on the information received from three foreign FIUs, it was concluded that the bank statement for cash withdrawal was forged. The case was further referred to the SAO.

SAO confirmed that the banking documentation was false and that the agreement between the suspected person and the company was formalised prior to the establishment of such company and was not actually signed by the suspected person.

Eventually, the Financial Inspectorate imposed a fine of HRK 45 000 (EUR 6 000), but the SAO dismissed the case because of the lack of sufficient elements to prove the illicit origin of the money.

246. Croatian authorities indicated that they conduct parallel financial investigations routinely establishing the proceeds of crime and enabling freezing, seizure and confiscation of the assets. In addition, several case studies have been presented where proceeds were identified through parallel financial investigations and later seized and confiscated. However, the exact number of parallel financial investigations remains unclear since they are conducted in the framework of criminal investigations of the predicate offence. In general, parallel financial investigations are used mainly for the purpose of establishing the proceeds that are directly linked to the predicate offences and not to trigger ML investigations and, in the assessment team's view, it is due to a number of reasons, as explained below.

247. The lack of full administrative capacities in the SAO has been recognised in the NRA since there have been no permanent financial investigators employed so far (authorities indicated that the SAO sometimes engage temporary investigators from other authorities, such as the tax authority) and the Department for the Investigation of Proceeds from Crime has not become operational yet. It remains difficult to attract qualified candidates for specialised financial investigators because of uncompetitive employment conditions. The lack of financial specialists has negative repercussions on the ability of the SAO to fight against economic and financial crime since these investigators were meant to assist state attorneys in analysing complex financial data.[130]

248. In addition, tracing money and proceeds of crime is not a general high–level policy objective of the investigations particularly in relation to indirect proceeds of crime. Case law does not properly incentivise to allocate the necessary resources to proceed with ML charges because the sentence would be essentially the same if defendants were only prosecuted for the predicate offence (see the analysis of ML sanctions below).

249. For instance, a financial investigation did not trigger ML investigation in relation to some Croatian nationals and foreigners who were found to be related to a case of international drug trafficking of around 100 kg of cocaine from South America where the transportation of drug was done from a Croatian port with the aim to distribute the drug in EU countries. Amongst other reasons pointed out by some Croatian authorities, the drug found in the vessel had not been sold yet, and therefore, they considered that an ML case could not be launched.

250. The high evidentiary thresholds described above usually causes authorities to transfer the case to third countries where the predicate crime occurred. Croatian authorities affirmed that the proceeding is transferred in cases when the predicate crime occurred in a foreign country, and the foreign country does not co–operate, but it was not firmly confirmed by the presented cases, such as the "La Familia" case. Authorities did not pursue ML offence in this case, yet it was instead transferred to the foreign jurisdiction even the predicate crime was not committed in that country.

251. Special investigative actions (i.e., interception of communications, controlled deliveries) are undertaken particularly in cases of drug trafficking, but also in relation to other serious

[130] European Commission 2020 Rule of Law Report Country Chapter on the rule of law situation in Croatia, p.6.

offences. The Croatian authorities use these investigative actions in order to establish the predicate offence, which often is not accompanied by the prosecution of the associated ML.

**Box N°3.14: Case example of co–operation**

On 20.08.2018 foreign company made a payment in the amount of USD 136,750.09 to the account of the Croatian company. Immediately upon the receipt of the notification, the national police requested the AMLO to perform its activities. The result was that the payment was not made to the company in Croatia but was returned to the payer on the same day.

The transaction was subject to a criminal investigation conducted by the police in 2018 and 2019, in coordination with the USKOK and in co–operation with the AMLO, against an international organised criminal group that was committing financial frauds and money laundering. The criminal investigation, which involved special investigation techniques and bank transaction analyses, established that one of the suspects, by himself or through other suspects, assumed real management of several companies headquartered in Croatia, in the ownership or under the control of the suspects. After several foreign companies had made payments to the accounts of the Croatian company in the amount of at least EUR 3.2 mln. and GBP 680,000 originating from Business Email Compromise (BEC) frauds, most of these financial means were further transferred to accounts of companies from different countries. In addition, international police co–operation took place. As a result, USKOK conducted an investigation against six Croatian nationals and two foreigners for ML offence.

252. The SAO advised that when executing incoming MLA requests, they consider whether there are grounds that an ML offence was committed. Some cases were presented where information from MLA requests contributed to ongoing domestic ML investigations. However, authorities did not present any ML investigation initiated solely based on information from incoming MLA requests.

**Box N°3.15: Examples of the MLA request used in domestic proceedings**

In November 2014, the AMLO disseminated a case related to a Dutch citizen XY living in Croatia suspected to commit ML through Croatian bank accounts, real estate and vessels.

In June 2015, the SAO launched a criminal investigation against defendant XY for ML. During the investigation, the SAO interrogated numerous witnesses, obtained relevant documentation, and ordered the tax control of business operations of trade companies. Provisional measures against XY were also applied, and the SAO issued a European evidence warrant to obtain evidence from the proceedings conducted against XY in the Netherlands. Requested evidence was necessary to prove the "predicate criminal offence" committed in the Netherlands.

Additionally, the SAO received an EAW and a freezing order from Dutch authorities for the purpose of freezing bank accounts and property already frozen in the context of the Croatian criminal proceeding.

As there were parallel proceedings in Croatia and the Netherlands against the same person for connected offences, the coordination meeting was organised by Croatian and Dutch national members at the EUROJUST. It was decided to concentrate the proceedings in the Netherlands because the predicate offence was committed there, and Dutch authorities obtained enough evidence for proving the predicate offence.

After three years, XY was convicted in the Netherlands and frozen money in Croatia should be confiscated for the purpose of compensation of the injured party, but the procedure of the recognition and execution of the confiscation order has not yet been issued by the Dutch judicial authorities.

253. Additionally, authorities presented some examples where they initiated ML investigation, but upon receiving MLA request, due to the fact that the predicate crime was committed in the foreign country, no further domestic ML investigation was launched. The case was transferred to the foreign jurisdiction.

**Box N°3.16: ML case transferred to foreign jurisdiction**

In 2017, Croatian prosecutors investigated several persons for ML offence. At the same time, Italian prosecutors ordered the seizure of EUR1.5 mln. for the purpose of securing the proceeds of crime in the Republic of Croatia. The execution of the order was postponed since the domestic investigation was in progress, and the proceeds of crime had already been seized. SAO launched the investigation based on the STR, an order received by the Italian authorities and information on predicate offence obtained through the police co–operation. Since the defendants were detained in Italy prosecuted for a predicate offence committed on Italian territory, Croatian authorities transferred the case to Italy to be prosecuted for ML offence as well.

254. Croatian authorities consider plea bargaining a useful tool for gaining valuable co–operation of the defendant, who may provide evidence or testimony which can be used against others aiming for higher–level targets of criminal organisations. It has been applied in a relevant case of migrants smuggling and fraud also for this purpose and in the context of an ML case. As a result, in an ML case, three persons were convicted, and a legal person was liquidated in 2016.

255. The authorities advised that all the LEAs, TA, CA and the AMLO undertake some ML–related trainings. They all have experienced staff members, but some are facing under–staffing issues, e.g., as described above for the SAO and under IO.6 for the AMLO.

### *3.3.2. Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies*

256. Croatian authorities have indicated in their NRA that most proceed generating crimes are tax evasion (tax or customs duty evasion), drug crime (unauthorised production and trade in illicit drugs, enabling the use of illicit drugs), and corruption. These are followed by fraud, abuse of intellectual property rights, avoidance of customs control, trafficking in human beings and human smuggling, prostitution, embezzlement, and usury, as posing medium ML threat.

**Table 3.11: The number of indictments for predicate offences posing high ML threat**

| Type of the offence | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| **Tax evasion** | 55 | 64 | 138 | 100 | 130 | 141 |
| **Drug related offences** | 797 | 1016 | 937 | 716 | 888 | 915 |
| **Corruption related offences** | 469 | 339 | 226 | 290 | 208 | 225 |

257. Broadly speaking, it was apparent from the NRA and the discussions with authorities, that there has been a problem with the lack of statistics, and even once available, it is often inconsistent. In order to substantiate conclusions about the effectiveness of the system, the assessment team, in addition to provided figures, used case examples. Croatian authorities referred to some cases where predicate offences rated as high ML threat were investigated and prosecuted, particularly in relation to tax evasion, drug trafficking and corruption, as well as fraud, which is rated as medium ML threat.

**Table 3.12: Number of ML investigation per predicate offence**

| Year | Computer fraud | Fraud | Tax evasion | Corruption[131] | Forgery | TOTAL |
|---|---|---|---|---|---|---|
| **2015** | 3 | 1 | 1 | 1 | 0 | 6 |
| **2016** | 3 | 5 | 1 | 2 | 1 | 12 |
| **2017** | 2 | 1 | 2 | 0 | 0 | 5 |
| **2018** | 1 | 0 | 1 | 0 | 0 | 2 |
| **2019** | 2 | 1 | 0 | 0 | 2 | 5 |
| **2020** | 2 | 2 | 2 | 2 | 1 | 9 |

258. The number of ML investigations and prosecutions over the review period is modest and not fully in line with the country's risk profile (see Table under 7.1) despite some crimes being identified as posing a high ML threat. This conclusion is also supported by the majority of cases presented to the assessment team, where the focus is on the predicate offence and only to a limited extent on ML, as previously described.

259. The 2020 NRA reflects, to some extent, awareness of the authorities that the achieved results, particularly concerning tax crimes, are not consistent with the ML risks of the country, especially relatively low number of criminal proceedings for tax crime–associated ML "definitely points to significant problems in detection and prosecution of such unlawful conduct"[132]. ML is not being investigated in a sufficiently proactive manner, nor is it adequately reflected in the AML/CFT national policy. In addition, the 2020 NRA Action Plan does not include any action directly referred to LEAs or courts to address the problems of ML investigation, prosecution and conviction and consistency with the country's risk profile, despite the fact that the previous action plan had such measures envisaged. Notwithstanding, the impact of the implementation of the previous action plan is unclear. Therefore, no adequate measures have been envisaged to overcome these obstacles at the policy level.

260. Misuse of legal persons for ML purposes is pointed out as a relevant ML risk in the context of the 2020 NRA. Additionally, the Serious Organised Crime Threat Assessment for 2019 to 2020 conducted by the MoI contain an analysis of the methods for abuse of legal persons, using as a "façade of legality" (see the methods described under IO.5).

261. Despite all the methods of abusing legal persons, ML is not proactively pursued in connection with it. It is only prosecuted if a particular legal person holds significant amounts of proceeds of crime or has been used to generate those illicit funds. Front companies used for the purpose of ML are not prosecuted as a rule.

262. In order to assess the consistency of different ML types with the country's risk profile, authorities provided ML convictions. However, almost all of them referred to computer fraud, although the major ML threats in Croatia are corruption, tax evasion and drug trafficking. As

[131] All cases refer to the criminal offence of abuse of trust in business.
[132] Page 9, para. 3, of the 2020 NRA.

previously stated, some relevant investigations, prosecutions and convictions referred to these crimes were provided to the assessment team, but ML is not pursued on a systematic basis.

263. The 2020 NRA refers to the so–called "Balkan route" as an ML threat for Croatia to be used as a transit point for arms trafficking, trafficking in human beings, drug trafficking, etc. Although some relevant and complex cases prosecuting predicate offences in this context were presented to the assessment team, the country is focused on these predicate offences and is not taking a proactive approach concerning ML associated with the referred threat and, thus, only a limited number of ML investigations and prosecutions have been conducted during the assessment period concerning this phenomenon. The overall results in this area do not commensurate with the risks posed by the so–called "Balkan route".

264. Certain delays in criminal procedures of ML and other complex cases have been detected. Complex investigations are usually finished in a maximum term of 18 months by the SAO but, when the case is remitted to courts for judgement, it sometimes takes many years to receive a final decision of the Courts. The confirmation of the indictment also may last long, particularly in complex cases. In a specific significant case (see Gold case) an indictment has not been confirmed for more than two years, implying the release of the seized funds since exceeding the maximum legal term. According to the information provided, one of the main reasons for these undue delays relates to the structure of the intermediary stage of the criminal procedure. Defendants must be compulsory present before the court in a first hearing in order to declare themselves guilty or not, otherwise, a judgement *in absentia* must be judicially authorised. It is only authorised if there are particularly important reasons and a judgement in a foreign state and/or extradition is not possible, or the defendant is on the run or out of the reach of state bodies. The assessment team was informed that judicial criteria to authorise the *in–absentia* judgement is strict and that sometimes defendants would be acting in bad faith, particularly in cases with multiple defendants, refraining (alternatively and repeatedly) to attend the initial public hearing in order to postpone it, as well as to postpone the decision of the court.

265. Additionally, undue delays might be caused to some extent by the ethical performance of the judges. Judges have been charged with the violations of impartiality and improper gifts received from the suspect in the criminal case[133]. Further, three judges were arrested in relation to the alleged corruption offences. It is to be noted that the President of the relevant Court also requested a new security check regarding the judges dealing with corruption and organised crime cases at that court.

### *3.3.3. Types of ML cases pursued*

266. Competent SAO and USKOK have the authority to investigate and prosecute a wide range of ML offences, including self–laundering, third–party ML and stand–alone ML. The following table identifies achieved ML convictions by type:

[133] European Commission 2021 Rule of Law Report Country Chapter on the rule of law situation in Croatia, p.6

**Table 3.13: Different types of ML convictions[134]**

| Year | Total | Self–laundering | Third party ML | Foreign predicate offences |
|---|---|---|---|---|
| **2015** | 4 | – | 4 | – |
| **2016** | 8 | – | 8 | 4 |
| **2017** | 9 | 3 | 6 | 1 |
| **2018** | 6 | 2 | 4 | 3 |
| **2019** | 5 | 1 | 4 | 1 |
| **2020** | 6 | 5 | – | 1 |

267. There were no comprehensive statistics on the investigations and prosecutions by types of ML, and the AT drew its conclusions based on the statistics on convictions, as well as on the cases presented by the authorities.

268. Authorities indicated that conviction for predicate offence is not a prerequisite to convict for ML, and autonomous ML offence can be pursued without obstacles. However, the high–level evidentiary threshold, as explained above, poses concerns about the effectiveness to prosecute the autonomous ML offence. The LEA and judiciary explained that, in practice, there should be a precise link between the laundered money and exact predicate crime to pursue ML investigation/prosecution. Convictions presented as autonomous ML are mainly simple cases, mostly related to the laundering of the proceeds of fraud or internet fraud committed abroad. Despite the fact that a great threat is posed by international drug trafficking, there have been no autonomous ML convictions where laundered proceed could potentially be linked with drugs. The same conclusion can be drawn for corruption, as well as tax evasion.

269. Authorities have presented several cases of self–laundering as a type of ML offence. They are mostly related to some cases of fraud. However, achieving those types of convictions is affected by the strict interpretation of the ML offence (see explanation above: Supreme Court Judgements).

270. There have been some third–party ML convictions. However, those cases are also related to the laundering of proceeds obtained by fraud and internet fraud. Taking into consideration the risk and context of Croatia, especially misuse of the legal persons for ML purposes, more cases of third–party ML should be expected.

271. Furthermore, ML cases concerning proceeds of crime committed abroad are only pursued to a limited extent. Prosecutors usually transfer the case to the foreign jurisdiction where predicate offence has occurred. Authorities argued that this is done in order to secure illicit proceeds (which can be seized for two years only), since foreign jurisdictions do not provide timely assistance. However, in the view of the AT this argument is not supported by the number of outgoing MLA/EIO requests for ML offence (see IO.2).

272. The 2020 NRA has recognised that the misuse of legal persons is a relevant ML typology. Authorities identified typologies that indicate that this trend was in use for several years. However, legal persons are rarely pursued in the context of ML cases (see Core Issue 7.2). Croatian authorities affirmed that this is because most of these legal persons used for ML purposes are companies with no assets or activity or do not exist anymore when the investigation

[134] Statistics included in the MEQ non–consistent with other statistics on ML convictions provided by Croatian authorities.

is launched, but this fact could only explain partly the very limited number of cases (see IO.1 and IO.5).

273. In conclusion, almost all final ML convictions presented to the assessment team were simple ML cases where predicate crime committed abroad was fraud and computer fraud and the money was further transferred to the bank accounts of the Croatian citizens.

**Box N°3.17 The most complex ML conviction**

The criminal investigation against eight natural and three legal persons for money laundering offence was triggered by the AMLO dissemination in 2014. Predicate offences were economic crime and counterfeiting of documents. Namely, defendants issued fictitious invoices regarding mutual purchase and sale businesses and transferred money based on it. Based on a false travel document of the natural person, who was the director of the company, tried to cash the funds from the company's account in a bank. The total amount of the laundered property was around EUR 110 000. During 2017 and 2018, all defendants were convicted with a suspended imprisonment penalty.

### *3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions*

274. Criminal sanctions under the technical compliance (c.3.10) are assessed as not being proportionate and dissuasive. Furthermore, even applied sanctions, in practice, for ML are not sufficiently effective or dissuasive since they are minimal and not proportionate to the seriousness of the crime and its associated risk in Croatia. Imprisonment penalties are, in the majority of cases suspended and rarely effectively applied. It is positive that the 2020 NRA is aware of this situation, but no measures were included in its Action Plan to remedy this deficiency.

275. The legal range of imprisonment is from six months to five (or even eight) years, but the average imprisonment penalty applied for ML varies between is 6.6 months (2017) and 10.1 months (2015). Additionally, all imprisonment penalties were suspended except one (18 months of imprisonment were imposed, being only 10 months suspended). Although a fine is not established for ML, some minor fines were imposed in ML offences as an ancillary sanction. Since legal persons are rarely investigated and prosecuted, only one conviction was presented to the assessment team. The imposed sanction was liquidation of the legal person without any fine. This sanctioning regime cannot be assessed as proportionate.

276. The table below presents a summary of all sanctions imposed in the final ML judgements provided to the assessment team.

**Table 3.14: Sanctions for ML offence**

| Case no | Year | Legal person (LP)/ Natural person (NP) | Proceeds laundered (EUR) | Sentence applied |
|---|---|---|---|---|
| KO 1035/19 | 2014 | 2 NP | 34.016,66 | Suspended sentence |
| K.367/14–26 | 2015 | NP | 6.304,13 | Suspended sentence |
| 23 ko 1526/14 | 2015 | 2NP | 9.629,20 | Suspended sentence |
| K. 1465/15–2 | 2015 | NP | 18.733,33 | Suspended sentence |
| K 935/2016–18 | 2016 | 3 NP<br>1 LP | 9.333,33 | Community service<br>Liquidation of the legal person |
| 6.673/15–16 | 2016 | NP | 3.881,00 | Suspended sentence |

| | | | | |
|---|---|---|---|---|
| K. 491/14–19 | 2016 | NP | 12.575,86 | Community service |
| Kov. 36/17–7 | 2017 | Np | 122.000,00 | Community service |
| K 824/15–11 | 2017 | N | 2.306,66 | Suspended sentence |
| Kov. 57/2015–71 | 2017 | 2N | 27.537,18 | Suspended sentence |
| 19K–16/17–2 | 2017 | NP | 4.266,66 | Suspended sentence |
| K 452/17–2 | 2017 | NP | 800,00 | Suspended sentence |
| K 120/2019–4 | 2018 | 2 NP | 27.537,18 | Suspended sentence |
| K. 694/2018 | 2018 | NP | 27.537,18 | Suspended sentence and fine 8 428,57 EUR |
| K. 1904/17–81 | 2018 | 2NP | 248.000,00 | Suspended sentence |
| K 119–16 | 2018 | NP | 3.693,86 | Suspended sentence and fine 906,60 EUR |
| K 55/2018 | 2018 | NP | 79.355,22 | Suspended sentence |
| K. 7/2018 | 2018 | NP | 79.355,22 | Suspended sentence and fine 6.623,00 EUR |
| K.2215/16–43 | 2020 | NP | 44.863,33 | 3 years |
| k. 1522/20–22 | 2020 | NP | 38. 640. 235,67 | 1 year 6 months imprisonment |

277. The NRA pointed out the low level of sanctions imposed by Courts for ML, stating that the level of sanctions is closer to 1/3 of the statutory prison sentence. As referred above, the level of sanctions is even lesser, and penalties are generally being suspended. The NRA also indicated that penalties imposed by judges had not been intensified despite the appeals filed by the SOA, concluding that the criminal sanctions applied, in practice, remain disproportionate to the legislator's sentencing policy for ML.

278. It is a matter of concern to the assessment team the extent to which the protected value damaged by ML offence is understood in Croatia, given the low sanctions imposed for ML and also the acquittals grounds used by courts in some cases.

### *3.3.5. Use of alternative measures*

279. The assessment team when discussing with the police officers and state prosecutors explored that several alternative measures were applied in circumstances where ML conviction was not possible to secure.

280. Prosecution of the predicate crime and tracing proceeds of crime for the purpose of confiscation is the main focus of the Croatian authorities, as was explained in paragraphs above (e.g., see case exampled in Box N° 3.12). Thus, primarily because of the high evidentiary threshold for ML offence, authorities pursue predicate criminal offence and direct proceeds of crime.

281. Croatian authorities also highlighted several case studies where a considerable amount of drugs was seized by working with international partners in which way they disrupted potential ML activity.

282. Croatia has a legal basis for alternative measures in cases where it is not possible to secure ML conviction to some extent. Notwithstanding, Non–conviction–based confiscation (NCBC) has been applied only once but not to an ML related case, mainly due to NCBC limited scope and also, to a minor extent, to its limited understanding of by the LEA and judiciary. It seems that NCBC is not a regular alternative measure when a proceeding *in absentia* is rejected by Courts.

283. NCBC is possible under the Croatian legislation (Art. 560A of the CPC), but it only applies if the defendant is dead, permanently incapable of arguing or not available to judicial authorities. NCBC is not applicable in those cases where the conviction cannot be secured because of formal

reasons (e.g., the statute of limitations has been exceeded), even if the criminal origin of the proceeds is proven. The standard of proof required to confiscate assets following an NCBC is the same as needed to convict in a regular criminal proceeding and, therefore, the reversal of the burden of proof does not apply for in rem confiscation.

*Overall conclusions on IO.7*

284. Croatia has extensive powers to identify, investigate and prosecute ML. Despite the clear legislation which is mostly in line with the international standards, understanding of the ML offence by the judiciary is limited. The actual results (investigations, prosecutions, and convictions for ML offence) are achieved to a negligible extent since the focus is on the establishment of the predicate offences.

285. While predicate offences posing high ML threat have been effectively investigated, prosecuted and convicted, tracing money and proceeds of crime for the purpose of identifying ML offence is not a high–level policy objective. There is no proactive approach applied, especially when foreign proceeds are detected, and legal persons abused.

286. Croatia pursues different types of ML but to a limited extent. The ML convictions obtained in the review period do not mitigate the risks since almost none of the presented cases are related to the three major–posing threats in Croatia. It was observed that after the indictment, undue delays in criminal procedures for complex cases of ML and predicate offences occur, which have a negative impact on the overall achieved results. In addition, criminal sanctions applied, in practice, for ML are not sufficiently effective or dissuasive since they are minimal and not proportionate to the gravity of the crime and its associated risk in Croatia.

287. **Croatia is rated as having a low level of effectiveness for IO.7.**

## 3.4. Immediate Outcome 8 (Confiscation)

288. Croatia has a legal framework on freezing, seizing and confiscation of instrumentalities and proceeds of crimes, confiscation of equivalent value, as well as extended confiscation. The Croatian legal system also provides for a non–conviction–based confiscation.

289. The CPC requires the SAO to determine proceeds of crime when there are grounds for suspicion that proceeds generating crime has been committed. The SAO may be assisted by the Police and the competent administrative bodies of the MoF when proceeds of crime are suspected to be of great value (Art. 206i of the CPC).

### *3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective*

290. Confiscation of proceeds, instrumentalities and property of equivalent value is pursued as a policy objective to some extent in Croatia.

291. Croatian authorities consider that the 2020 NRA Action Plan serves as a general policy document for the confiscation of proceeds of crime. In the 2016 NRA, one of the main goals was to successfully confiscate the proceeds of crime. This was followed by specific measures included in the 2016 NRA Action Plan with the aim to strengthen the confiscation regime. Notwithstanding, the report on the implementation of the 2016 Action Plan pointed out only general figures on the achieved results in seizure and confiscation, as well as the observation that capacity–building measures were not implemented. On the other hand, the main focus of the 2020 NRA is on the

effective use of available resources in the AML/CFT regime and the prevention of the abuse of the Croatian financial and non–financial system for concealment of criminal proceeds. Furthermore, the 2020 NRA Action plan only includes one measure directly related to confiscation ("Employment of financial investigators in the SAO in the Departments for Investigation of Criminal Proceeds") but does not include any unachieved measures from the previous Action Plan, neither does it address identified vulnerabilities in the NRA regarding seizure and confiscation. Therefore, the assessment team is of the opinion that the new 2020 NRA Action Plan is not adequate to properly address deficiencies identified in the confiscation procedure. (See also the opinion of the AT on the Action Plan under IO.1)

292. Confiscation of proceeds, instrumentalities and funds related to TF has not been identified as a policy objective either in the NRA or in the Counter terrorism strategy. However, this strategy refers to the financial investigations for the purpose to "seize proceeds of crime and to seize any form of proceeds of crime from natural and legal persons connected with terrorist activities". In the view of the assessment team, this is not a comprehensive approach and is caused by the lack of understanding of the TF risk in the country (see IO.9).

293. Authorities systematically conduct parallel financial investigations as part of investigation of predicate offence in order to seize and confiscate proceeds. LEAs and the AMLO regularly initiate measures for securing assets once they are identified, which are followed up by the court's orders (for the AMLO's actions, see IO.6). Yet, the focus remains on the suspension, seizure, and confiscation of the proceeds of the predicate offences committed in Croatia (for example, tax crime, drug trafficking, etc.). Nevertheless, proceeds of foreign offences are not pursued proactively by Croatian authorities, which is not in line with the risk profile of the country (according to the Croatian authorities, this is also caused by inadequate co–operation of foreign countries). Croatian authorities stated that financial investigations are regularly led as part of criminal investigations with the aim to determine the proceeds of crime. However, the exact number, as well as the outcomes of those investigations were not presented to the AT and therefore, the conclusion could not be drawn on the effectiveness of this legal instrument vis a vis predicate offence. In addition, the authorities do not have comprehensive guidelines which would instruct them how to effectively use different sources of information and conduct parallel financial investigations. Croatian authorities provided a Handbook regarding prevention and the prosecution of ML (August 2020) used for training purposes mainly. The Handbook includes chapters on "criminal prosecution of the perpetrator for the criminal offence of ML" and "prosecution of perpetrators of ML, in practice". Nevertheless, this Handbook is a general didactic material and does not establish specific protocols or actions that should be undertaken when conducting parallel financial investigations.

294. Croatian LEAs trace instrumentalities used for the commission of the criminal offence. However, there are certain limitations, as described under R.4(c. 4.1) preventing the LEAs from successful confiscation of instrumentalities intended for the use in committing criminal offence and confiscation of equivalent value of instrumentalities. Authorities did not provide statistics on the seizure and confiscation of the instrumentalities, but from the case examples presented to the assessment team, it seems that they regularly secure instrumentalities once they find these and further confiscate.

295. Authorities suggested that confiscation of property of equivalent value is regularly ordered in convictions when proceeds were not previously secured. The authorities generally explained the application of this legal instrument and presented some cases, but no statistics were provided

to the assessment team. This prevents the AT from drawing a firm conclusion on the effective execution of the orders for confiscation of property of equivalent value.

### *3.4.2. Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad*

296. Confiscation of proceeds in Croatia has a subsidiary nature since legislation gives priority to restitution to victims. Croatian authorities confirmed that once victims are compensated, the confiscation of remaining assets can be ordered. According to the 2020 NRA, in 82% of the proceeds generating offences (mostly for crimes against property, crimes against the economy, corruption, crimes against computer systems, intellectual property crimes), victims were compensated pursuant to their civil claim. However, Croatia does not keep comprehensive statistics on the compensation orders, and therefore, the exact figures or estimates of the value of the proceeds of crime remain unknown.

297. The effectiveness of the confiscation in relation to the domestic proceeds generating predicate offences has been achieved to some extent. The SAO has provided statistics on seized and confiscated assets to illustrate the effectiveness of these measures, yet most of the property is related to fraud. In addition, in the assessment period, no significant proceeds of ML offences have been seized or confiscated. Regarding TF there has been no seizure or confiscation so far since Croatia did not investigate any TF cases (see IO.9).

298. In the table below, statistics present seizure and confiscation of proceeds, and according to the information provided by the country, it refers only to the cases for the offences committed domestically. There have been no specific statistics on the confiscation of foreign proceeds in domestic cases. However, some case examples were presented to the assessment team, such as the La Familia case (see IO.7), where the proceeds of crime have been frozen and afterwards confiscated in the neighbouring country following the MLA request of Croatia. Agreement between two countries led to the share of property, based on Warsaw Convention.

**Table 3.15: Value of frozen and confiscated assets in domestic cases (Source: SAO[135])**

| Offence | Year | Frozen/seized assets (in mln. EUR) | Confiscated proceeds of crime (in mln. EUR) |
|---|---|---|---|
| ML | **2015** | 4,99 | – |
| | **2016** | 7,90 | 0,069 |
| | **2017** | 0,54 | 0,0001 |
| | **2018** | 1,62 | 0,031 |
| | **2019** | 2,38 | – |
| | **2020** | 1,10 | – |
| Other predicate offence | **2015** | 6,24 | 13,14 |
| | **2016** | 7,58 | 37,48 |
| | **2017** | 64.21 | 10,92 |
| | **2018** | 3,80 | 19,44 |
| | **2019** | 7,03 | 14,84 |
| | **2020** | 6,83 | 19,23 |

299. As can be observed from the figures included in the table above, the ratio between seized and confiscated assets related to ML is considerable. ML–associated confiscations are incidental.

[135] The Ministry of Justice (MoJ) provided statistics for the same matter but informed about problems in gathering the relevant data. In any case, inconsistencies between statistics provided by MoJ and SAO are huge. This data is also inconsistent with the NRA information.

This is partly due to the fact that even in a limited number of ML investigations, the charges are later dismissed, and focus is on the predicate offences. This gap is also caused by the undue delays of ML–related criminal proceedings, which sometimes leads to releasing of seized property. (For details on ML investigations and prosecutions, see IO.7)

300. Legislation provides for the assets to be temporarily seized for a maximum term of two years until the indictment is confirmed by the Court. Indictments are not usually confirmed in the set period, especially in the complex cases, and therefore, seized assets are released, which makes further asset recovery impossible, and ultimately this does not make crime unprofitable. The authorities presented some cases where the investigation was conducted (and the indictment was issued) in the general term of 18 months, but the process to confirm (or not) the indictment before the Courts lasted more than six months, or even more than the investigation itself.

**Box N° 3.18: Gold case**

This previously referred complex case was launched in 2016. The indictment was issued in December 2017 (USKOK indicted 15 persons for tax crime) and was confirmed in December 2019 (two years after the end of the investigation). The final judgement of the case is still pending.

In this case, a total amount of HRK 8 680 383 (EUR 1 154 306) was temporarily blocked, but the larger part of the frozen property was finally released due to the expiration of the maximum deadline of two years.

301. Croatian authorities stated that the difference between seized and confiscated property in ML cases is also due to the transfer of criminal proceedings, and therefore, the previously seized property is confiscated in or by a foreign country and executed in Croatia. However, statistics in those cases have not been provided, nor has the estimation of the value of property related to those cases.

302. This discrepancy is also observed in relation to predicate crimes but in the opposite direction. Namely, the value of confiscated assets is higher than the value of seized assets. Based on the provided information in 83% of the cases, confiscation orders are applied without previously ordering the seizure of assets[136]. Furthermore, temporary freezing orders were issued in only 18% of cases where proceeds of crime were investigated. This discrepancy is partly caused by the fact that not all confiscated assets have been previously restrained. Croatian authorities also indicated that part of the confiscated assets has been compensated to victims.

303. Croatian authorities provided statistics including all confiscated assets, regardless of whether they were effectively recovered and enforced. In cases where prior provisional measures have not been adopted, the defendant is required to voluntarily comply with the confiscation order within 15 days after the final conviction. If confiscation is not duly accomplished, the case is referred to the SAO to undertake necessary measures for a successful and effective confiscation. Once the deadline for the recovery of the proceeds expires, the SAO launches an enforcement procedure that is often hampered by the fact that the defendants do not have any income or assets in their name. In the view of the assessment team, this is caused by the lack of sound strategy to trace proceeds, especially abroad and the lack of capacities in terms of financial investigators.

[136] 2020 National Risk Assessment, page 36.

304. Authorities argued that financial investigations are regularly conducted to trace proceeds and secure confiscation. In addition, several case studies have been presented where proceeds were identified through parallel financial investigations and later seized and confiscated. However, the exact number of the parallel financial investigations remains unclear since they are conducted in the framework of the criminal investigations of the predicate offence. Inter–agency co–operation in financial investigations is set on a case–by–case basis. Furthermore, law on the SAO provides the possibility to establish the Department for Investigation of Proceeds from Crime. However, this department has not been set up since 2014. Namely, although General State Attorney took a decision to establish departments for the investigation of proceeds of crime in Split, Rijeka, Zagreb and Osijek, they have not been yet operational. In the opinion of some Croatian authorities, it is mainly due to the working conditions of the position of financial investigator and the requirement of high professional standards disproportionate to the position's wage.

305. Croatia has established an Asset Recovery Office (ARO) to facilitate the tracing and identification of proceeds of crime and other crime–related property. Economic Crime and Corruption Department of the PNUSKOK is the national contact point for the submission of requests and the exchange of data between the national and foreign authorities for the purpose of tracing and identification of proceeds of crime (ARO). This Department of the PNUSKOK is regularly tracing and identifying proceeds of crime, but it is not specifically used as the ARO in national financial investigations since it was not widely known amongst the relevant practitioners and is primarily used in the context of international co–operation (see IO.2). Croatian authorities indicated that the Police Department where the ARO has been established is, in practice, developing all ARO's functions in the framework of its general duties.

306. Temporarily seized and confiscated assets are managed and preserved by the MPPCSA. Croatian authorities have shown consolidated experience in managing a wide range of property, such as precious metals, art and paintings, cars, etc., including the possibility to sell and transfer property, rent it or use it for public interest or social purposes, especially vehicles. Since investigations and prosecutions of legal persons are rarely conducted, management of seized companies has not been applied. Authorities explained that in the event the legal persons are seized, since there is no clear institutional and legislative framework set, they would not be able to manage it. Nevertheless, they suggested that the appointment of an ad hoc judicial administrator would be a solution to overcome this obstacle once the legal person is seized.

**Table 3.16: Seized and confiscated assets EUR preserved/managed by the MPPCSA; 2015–2020 (Source: MPPCSA)**

| | Assets | Number of orders | Value (EUR) |
|---|---|---|---|
| Freezing | **Cash** | 1863 | 13 111,64 |
| | **Movable property** | 47 | 1 661 110,64 |
| | **Real Estate** | 54 | 8 917 905,33 |
| | **TOTAL** | **1964** | **23 606 335,22** |
| Confiscation | **Cash** | 1935 | 32 017 137,24 |
| | **Movable property** | 97 | 56 562,65 |
| | **Real Estate** | 6 | 1 490 309,24 |
| | **TOTAL** | 2038 | 33 564 009,13 |

307. While to a limited extend, Croatia demonstrated to apply extended confiscation. For instance, in a case where a public officer was convicted for corruption (e.g., accepting bribes of

more than HRK 150 000 (EUR 20 000)), an extended confiscation of HRK 5 738 898 (EUR 765 186) was applied since the value of his property is disproportionate to his lawful income. This judgement was rendered in October 2019 and is not final yet, even though the events occurred between 2005 to 2009.

308. Regarding asset sharing with EU Member States, the Act on Co–operation in Criminal Matters with the Member States of the European Union serves as a basis for the country's policy in this context. Regarding the non– EU countries, assets can be shared if there is an agreement or international standard such as Warsaw Convention. Authorities did not present the statistics of the cases where asset sharing was applied with non–EU Member State, but some case examples were provided (see explanation under Core Issue 8.2).

309. Croatia also executed freezing and confiscation orders issued by foreign EU counterparts, as shown in the following table.

**Table 3.17: Freezing and confiscation orders received from and sent to EU counterparts.**

| Year | | Received orders/requests | | Issued requests (#) | |
|---|---|---|---|---|---|
| | | Freezing order (FO) (Amount in EUR) | Confiscation order (CO) (Amount in EUR) | FO | CO |
| 2015 | ML | 4 406 691 | | | |
| | Predicate offences | | | | |
| 2016 | ML | 2 112 967,86 | | | |
| | Predicate offences | | 100 000 | | |
| 2017 | ML | 55 398 | | | |
| | Predicate offences | 6 329 625,2 | | 1 | |
| 2018 | ML | 1 248 245 | 972 000 | | |
| | Predicate offences | 5 888 797 | | | |
| 2019 | ML | 21 428 687,8 | 4 000 000 | 2 | |
| | Predicate offences | 6 968 557,66 | 436 842,85 | 2 | |
| 2020 | ML | 21 562 739,34 | | | |
| | Predicate offences | 519 088,00 | 428 000,00 | 1 | |

310. There have been no seizure or confiscation of proceeds related to TF (see IO 9).

### *3.4.3. Confiscation of falsely or undeclared cross–border transaction of currency/BNI*

311. Croatia borders with EU and non–EU countries, but it does not participate in the Schengen Area (see Chapter 1). The country has several international airports and seaports. For the transportation of cash and BNIs, Croatia has introduced a written declaration system (see R.32). Controls are in place at the borders with non–EU countries, as well as at the international airports and seaports. However, the borders with the EU are controlled by the CA's mobile units used on a case–by–case basis. Mobile units are part of the CA and have the power to search persons and vehicles and then report to the Police any suspicion with regard to cash and BNI transportation, which can be directly seized by the CA's officers. The CA do not have the power to seize weapons, explosives, and dangerous materials, yet they report to the Police, who are entitled to undertake further measures. The assessment team is of the opinion that the CA and Police do have extensive co–operation in this regard.

312. The use of cash and its transportation is not identified by the 2020 NRA as a relevant ML/TF threat, rather, it points out that the use of cash poses difficulties to trace proceeds of crime. However, some criminal cases presented to the assessment team were related to the use of cash (e.g., I–typology). In the view of the assessment team, this, together with the nature of the so–called "Balkan route" (used for drug trafficking) (e.g., case "La Familia"), suggests that illicit cross border transportation of cash may be a significant ML/TF threat in Croatia. This conclusion is supported by the fact that a large part of the Croatian border is also an external border of the EU. In addition, the AMLO identified high cash payments of an unknown source as one of the current and future Croatian ML threats. Besides this, the EU supranational risk assessment also considers cash and cash–like assets one of the main European ML risks.

313. The CA is the leading authority to monitor cross–border transportation of cash. It applies a variety of red flags and tactics to detect illicit transportation of cash. Although comprehensive statistics were not provided by Croatian authorities, it was indicated that some of the tactics used are targeted controls on cross–border transportation of cash. They are regularly conducted at the Croatian borders with non–EU jurisdictions (i.e., ports, airports, and roads). Some examples of the red flags applied by authorities are: collecting information on passengers, their departure/destination, means of transport. All that information is used during controls to determine the undeclared cash. In case of undeclared or falsely declared cash, the CA, as well as some other authorities (i.e., Police), are empowered to initiate a misdemeanour procedure.

314. When a breach is detected, cash is restrained, and the case is submitted to the Financial Inspectorate for sanctioning purposes. The administrative sanctions applied for undeclared cash are per se modest (between HRK 5 000 – 50 000 (EUR 670 – 6 70)), especially in relation to high amounts of undeclared assets. Since this sanction from 2018 is not followed by confiscation of the transported cash, it is not dissuasive[137].

**Table 3.18: Cross–border transportation of cash/BNI: fines, assets restrained and confiscated[138]**

| Year | Number of reports | Assets restrained (EUR) | Fines (EUR) | Confiscated assets (EUR) | Returned assets (EUR) |
|---|---|---|---|---|---|
| **2015** | 10 | 415 568 | 32 666,66 | 76 133 | 464 600<br>6 600 * |
| **2016** | 13 | 288 945 | 31 333,33 | 24 000 | 730 984 |
| **2017** | 11 | 581 545 | 23733,33 | 21 350 | 406 553 |
| **2018** | 11 | 255 831 | 19 066,66 | 16 180 | 514 688 |
| **2019** | 12 | 260 136,23<br>612 000,00 * | 28 533,00 | 0 | 410 303,23 |
| **2020** | 9 | 532 621,50 | 23 333,00 | 0 | 495 569,00 |

315. Information on cross–border declarations of cash is sent to the AMLO when ML suspicions are detected, being used in their analysis as any other source of information. When an

[137] According to provided information, on 7 May 2021, the Foreign Currency Act was amended in order to implement the 2018 EU Cash Control Regulation, but this new law entered into force after the on–site visit. The Amendments abolished confiscation as a sanction for the administrative offence of failing to declare cash exceeding EUR 10 000 when entering or leaving the European Union through Croatia. The new maximum amount of fine has been increased to HRK 100 000 (EUR 13 400) and to HRK 1 000 000 (EUR 134 000) for aggravated forms. The Amendments, however, provide that the fine must be lower than 60% of undeclared cash.

[138] Based on the information included in the NRA, which sometimes is not consistent with the statistics provided in the MEQ.

administrative breach is detected, the CA conducts some basic checks (e.g., interview with the holder of the cash, search in his/her luggage, analysis of his/her personal documents and those related to the origin or the destination of the cash, etc.). In this context, the following statistics were provided (BNI–related declarations have not been filed, no TF suspicious have been reported):

**Table 3.19: Cross border transportation of currency**

| Year | Number of declarations | | ML suspicious |
|---|---|---|---|
| | Incoming | Outgoing | |
| **2015** | 214 | 54 | 2 |
| **2016** | 288 | 131 | – |
| **2017** | 256 | 126 | 3 |
| **2018** | 225 | 126 | 2 |
| **2019** | 117 | 54 | – |
| **2020** | N/A | N/A | N/A |

316. Cross–border cash controls rarely triggered any further criminal investigations, and thus, there is no correlative conviction–based confiscation of illegal property (cash). There is no generally established practice to analyse administrative infringements from a criminal perspective beyond the mere substantiation of the administrative sanctioning proceedings. Information on cross–border declarations is included in the AMLO's databases and used when conducting operational analysis.

317. In addition, case law of the ECHR emphasises that Croatian authorities, in case of undeclared cash, despite the red flag of the ML indicators, did not initiate any criminal charges. This judgement can serve as a base to support the assessment team's view on the lack of proactive approach of the LEA when undeclared cash has been revealed. Furthermore, ECHR concluded that Croatia should question the effectiveness of their sanctioning regime in this matter in a fair equilibrium with human rights and the ECHR's jurisprudence (e.g., Grifhorst v. France), including the possibility of broadening the scope of NCBC, and systematically investigate breaches of cross–border transportation of cash from a criminal and financial perspective.

**Box N° 3.19: Case B. v. Croatia (Judgement, of 31 January 2017, of the ECHR)**

Citizen B. of a neighbouring country entered Croatia and opened a bank account depositing a total amount of EUR 180 000 without declaring it to the CA (he made two cash deposits). The AMLO opened the case and initiated a misdemeanour proceeding. Citizen B stated that the money came from the sale of the business premises in country X, and he intended to buy real estate in country X but from the Croatian national. The vendor insisted on being paid from a Croatian bank account. In support of his claim, B provided a written copy of the contract of sale in respect of his business premises (it was sold two years before he entered Croatia) and a preliminary agreement relating to the purchase of the real estate in country X, but with the date that was two weeks after he entered Croatia. B was found guilty of the administrative offence fined HRK 10 000 (EUR 1 300), and the EUR 180 000 was confiscated. It was concluded that the evidence presented did not correspond to B's statements. Besides this, B had been unable to provide sufficient evidence to justify his earlier money transfers of EUR 882 900 to the vendor accounts in Tunisia and Jordan between 2005 and 2008.

The ECHR considered that, although the referred confiscation pursued a legitimate aim in the general interest (namely, the fight against money laundering), there was not a reasonable relationship of proportionality between the means employed by the authorities to achieve that

aim and the protection of B's right to the peaceful enjoyment of his possessions. The ECHR also considered that, despite the doubts concerning the legitimate origin and destination of the money referred by Croatian authorities, there was nothing to suggest that, by confiscating the amount of EUR 180 000 from B, the Croatian authorities sought to forestall any criminal activities, such as money laundering and the only illegal (but not criminal) conduct which was attributed to B in respect of the money was his failure to declare it to the CA. Moreover, the ECHR emphasized that B did not have a criminal record and was not charged with any criminal offence.

Finally, the ECHR considered that it had not been convincingly shown or indeed argued by the Croatian authorities that the fine alone was not sufficient to achieve the desired deterrent and punitive effect and prevent future breaches of the declaration requirement and, in these circumstances, the ECHR concludes that the confiscation of the entire amount of money that should have been declared, as an additional sanction to the fine was disproportionate.

This was not the first time the ECHR declared a violation of Art. 1 of Protocol No.1 to the Convention regarding the Republic of Croatia related to confiscation of undeclared cash at the borders for similar reasons (case Gabrić v. Croatia).

### *3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities*

318. The confiscation results achieved so far by Croatia do not appear to be entirely consistent with the level of ML/TF threat present in the country and national AML/CFT policies and priorities. According to the statistics provided approx. 56% of the confiscated property is related to fraud, and only 22% relates to corruption and bribe–taking. This is not consistent with the results of both NRAs from 2016 and 2020 since tax crime, drug trafficking and corruption are recognised to pose the highest threat. In addition, in the assessment period, there were no substantial ML cases, and consequently, no significant proceeds were seized or confiscated in ML–related cases.

**Table 3.20: Value of confiscations broken down by main offences in mln. EUR 2015–2020 (Source: SAO[139])**

| Offence | ML threat | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | Total |
|---|---|---|---|---|---|---|---|---|
| **ML** | – | – | 0,069 | 0,0001 | 0,031 | – | – | 0,10 |
| **Fraud** | Medium | 6,88 | 30,47 | 4,84 | 12,66 | 9,02 | 2,58 | 66,48 |
| **Corruption and bribe–taking** | High | 4,06 | 2,77 | 3,86 | 3,95 | 2,06 | 6,04 | 22,77 |
| **Drug trafficking** | High | 0,42 | 0,62 | 0,38 | 0,28 | 0,12 | 6,95 | 8,79 |
| **Tax offences** | High | 0,32 | 0,70 | 0,66 | 1,61 | 1,74 | 1,19 | 6,25 |
| **Participation in organised criminal association and racketeering** | – | 0,13 | 0,07 | 0,24 | 0,35 | 0,41 | 4,14 | 5,37 |
| **Robbery or theft** | Low | 0,43 | 0,55 | 0,52 | 0,32 | 0,17 | 0,76 | 2,78 |
| **Sexual exploitation** | Medium | 0,71 | 0,65 | 0,01 | 0,0003 | 0,005 | 0,00009 | 1,38 |

139The Ministry of Justice (MoJ) provided statistics for the same matter but informed about problems in gathering the relevant data. In any case, inconsistencies between statistics provided by MoJ and SAO are huge. This data is also inconsistent with the NRA information.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Trafficking in human beings and smuggling of migrants** | Medium | 0,019 | 0,07 | 0,12 | 0,22 | 0,12 | 0,019 | 0,58 |
| **Illicit trade in stolen goods** | – | 0,008 | 0,014 | 0,10 | 0,10 | 0,01 | 0,002 | 0,24 |
| **Smuggling** | Medium | 0,09 | – | 0,04 | 0,05 | 0,009 | 0,009 | 0,21 |

319. The table above confirms that ML–related confiscations are insignificant. In addition, smuggling of goods (particularly of tobacco) is a proceeds–generating crime with an associated medium ML threat (according to the 2020 NRA) but, smuggling–related confiscations are modest (e.g., none in 2016, less than EUR 10 000 in 2019 and 2020). In addition, fraud and robbery/theft were considered to pose medium and low ML threat, respectively, but, according to the data provided, fraud was by far the offence with a higher associated value of confiscated assets and large amounts of assets has also been confiscated concerning robbery/theft. There has been no TF–related confiscation since no investigation, prosecution, and conviction have been achieved so far (see IO 9). These confiscation results are not fully consistent with the level of ML threat present in the country and raise concerns as to whether it is consistent with the TF threat considering shortcomings in the risk assessment, as described under IO 1 and 9.

320. Risks related to cross border transportation of cash/BNI were not fully analysed by the NRA. While the outcomes of the border controls resulted in some concrete actions (i.e., fines and administrative confiscation of cash), they rarely triggered criminal investigations, hence never led to criminal confiscation.

### *Overall conclusions on IO.8*

321. Croatia does pursue confiscation as a policy objective to some extent. While there is no high policy document regarding confiscation, available legal instruments have been applied. Financial investigations are carried out when there are grounds for suspicion that proceeds generating crimes have been committed. In this regard, the authorities seize proceeds and instrumentalities once they find them.

322. Although significant proceeds of some predicate offences were confiscated, ML–related confiscation is not significant. Despite the results achieved so far, the confiscated amount is far inferior to the amounts seized both in ML and predicate offences and are not fully in line with the risk profile of the country.

323. Although authorities demonstrate experience in the management of almost all types of seized and confiscated assets (except legal persons), some seized assets have been released in significant cases because of undue delays in the proceedings before the court. The long–lasting of understaffing in the SAO also has a cascading effect on the overall results of confiscation.

324. Administrative sanctions applied for undeclared cash are per se low. These sanctions could be followed by confiscation of transported cash, but this was not applied since 2018, and the overall level of sanctions is not dissuasive.

325. Overall, major improvements are needed in order to make crime unprofitable.

326. **Croatia is rated as having a moderate level of effectiveness for IO.8.**

# 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

## 4.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 9***

a) Croatia has carried out a limited analysis of the TF risks. The authorities do not have a proper understanding of TF phenomenon and how different legal and illegal activities can be exploited for TF purposes. The country did not demonstrate that threat posed by FTF and their family members, migrant smuggling, the so–called "Balkan route", and OCG were properly analysed and assessed in the context of TF risks.

b) A number of preliminary inquiries potentially related to terrorism and terrorism financing have been conducted by LEAs, but these did not lead to any formal criminal or parallel financial investigations, and thus no prosecution and conviction for TF offence have been achieved so far in Croatia. While in certain instances, this is due to the lack of sufficient criminal grounds, in others, it is due to the lack of consideration of TF elements in specific cases.

c) Croatia has adopted a National Strategy for the Prevention and Suppression of Terrorism and the Action Plan. Some policy objectives are mentioned in this Strategy. However, only a general remark was made with respect to TF without specific and comprehensive actions concerning TF. Yet, there are no measures related to financial investigations.

d) In the absence of any conviction of TF, it is impossible to assess to what extent the sanctions applied would be proportionate and dissuasive.

***Immediate Outcome 10***

a) Croatia implements the UN TFS on TF relying on the EU framework, which does not ensure implementation of those "without delay". There is no national legal framework set to overcome this delay. No national framework is also set for identifying and designating persons and entities pursuant to UNSCRs 1267/1989 and 1988 and 1373. No procedures or mechanisms for de–listing or unfreezing assets are available publicly. The Standing Group did not demonstrate an active role in implementation of asset freezing requirements in the country.

b) Banks and other REs that are members of larger financial groups demonstrated sufficient understanding of TF–related UN TFS requirements. Tools for implementation of the TFS used by the most material REs ensure timely update and effective detection of matches. Smaller REs have weaknesses in understanding some requirements related to the frequency and the scope of checks. The current mechanism does not ensure immediate communication of additions and amendments to the sanctions lists to REs. Some outreach is provided to REs, but not sufficient guidance.

c) There were no funds or assets identified and frozen in Croatia pursuant to UN designations related to TF. Most REs demonstrated awareness of asset freezing

requirements. Several REs confirmed to have had false–positive matches with UN TFS listed persons. There was uncertainty among FIs and DNFBPs on the addressee of a report – the AMLO, MFEA, or MoI. This was because the MFEA, the designated authority for the receipt of freezing reports, did not demonstrate performing actively its role in implementation of asset freezing requirements in the country.

d) Croatia made efforts to conduct an assessment of risks in the NPO sector. The NPO sector was considered within the scope of the two NRAs conducted in 2016 (subject to ML vulnerabilities in the sector), 2020 (as a variable for assessment of the Country's TF vulnerabilities), and a thematic analysis by the Financial Inspectorate. None of these exercises led to identification of the subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse by virtue of their characteristics. This has affected the implementation of the targeted measures towards the sector and led to the lack of risk–based monitoring. A general AML/CFT outreach is conducted to the NPO sector, but not on NPO sector vulnerabilities for TF, and not reaching out to the donor community. The NPOs demonstrated no awareness that they could be abused for TF purposes.

e) Measures taken for implementing the UN TFS and preventing the abuse of the NPOs for TF purposes are not deemed adequate as they are affected by the limited overall understanding of the TF risks in the country, as demonstrated by authorities.

***Immediate Outcome 11***

a) Croatia implements the UN TFS on PF relying on the EU framework, which does not ensure implementation of those "without delay". There is no national legal framework set to overcome this delay. The MFEA does not demonstrate actively performing its role in implementation of the UN TFS.

b) There were no funds or assets identified and frozen in Croatia pursuant to UN designations related to PF. Most REs demonstrated awareness of asset freezing requirements. There were no real matches detected with the UN sanction lists on PF, but several REs confirmed to have had false–positive matches.

c) Banks and other REs that are members of larger financial groups demonstrated sufficient understanding of UN TFS requirements of PF. Tools for implementation of the TFS used by the most material REs ensure timely update and effective detection of matches. Smaller REs have weaknesses in understanding some requirements related to the frequency and the scope of checks. Some outreach is provided to REs, but not sufficient guidance.

d) Supervision of compliance with PF–related TFS is conducted within the scope of AML/CFT inspections, but there is a need for more frequent supervisory efforts focused on the weaker performing sectors and adequate resourcing. TA did not demonstrate to have guidance and to conduct TSF targeted inspections in the supervised REs.

***Recommended Actions***

***Immediate Outcome 9***

a) Croatia should: (i) conduct analysis of all cases where preliminary inquiries took place to detect potential challenges in pursuing TF investigations/prosecutions; (ii) proactively coordinate between the LEAs and SAO (setting agreement or MoU where necessary) to ensure all potential TF activities are identified, thoroughly analysed, investigated and prosecuted; (iii) develop a guideline drawing on international best practices on TF investigations and prosecutions, setting out the range of circumstances and sources of information (including MLA, EAW and other incoming data) to trigger TF investigations, and (iv) provide trainings to LEAs and judiciary.

b) LEAs should conduct parallel financial investigations systematically where a potential case of terrorism or terrorism financing is detected. Cases where family members are sending money or other assets to relatives in conflict areas potentially related to terrorism or terrorist organisations, should be investigated as potential TF cases.

c) Croatia should conduct a deeper assessment of TF risks, including national and sectorial vulnerabilities. TF risks posed by FTF and their family members, migrant smuggling, drug trafficking and OCG should be adequately analysed and assessed. This should be followed by outreach to raise TF risk awareness.

***Immediate Outcome 10***

Croatia should:

a) Establish a national framework for implementation of TF–related UN TFS measures by: (i) ensuring implementation of the UN TFS without delay; (ii) establishing formal mechanisms (e.g., providing the Government or Standing Group with respective powers), and developing formal, detailed procedures for proposing designations to the UNSC 1267/1989 and 1988 Committees, making domestic designations under UNSCRs 1373, de–listing of persons and unfreezing of assets.

b) Conduct an in–depth and comprehensive risk assessment of the NPO sector, with involvement of all relevant stakeholders and representatives of NPOs, to identify the subset of NPOs that may be vulnerable to TF abuse by virtue of their activities. Provide targeted outreach to NPOs and the donor community on potential vulnerabilities of NPOs to TF.

c) Establish: (i) clear mechanism or channel, and develop a reporting form, for submitting reports to MFEA on frozen assets or actions taken in compliance with the prohibition requirements, including attempted transactions by REs in line with the respective UNSCRs; and (iii) determine the recipient of these disclosures (contact point). Ensure that the MFEA's responsible recipient of disclosures has knowledge, powers and instructions for taking action upon the receipt of the disclosure from a RE. Ensure that all REs are made aware of information on reporting form, contact point and reporting channels, including that this information is publicly available.

d) Ensure immediate communication of the designations and further amendments in the TF–related UN TFS to the REs.

e) Provide clear guidance to REs, especially to DNFBPs, on their obligations under TF–related UNSCRs for freezing, unfreezing, reporting (included attempted transactions). Conduct further outreach to REs on their obligations.

f) Develop and implement a risk–based approach to NPO sector monitoring, provide sufficient supervisory resources and ensure termination of inactive NPOs.

***Immediate Outcome 11***

Croatia should:

a) Establish a national framework for implementation of PF–related UN TFS measures without delay.

b) Establish: (i) clear mechanism or channel, and develop a reporting form, for submitting reports to MFEA on frozen assets or actions taken in compliance with the prohibition requirements, including attempted transactions by REs in line with the respective UNSCRs; and (ii) determine the recipient of these disclosures (contact point). Ensure that the MFEA's responsible recipient of disclosures has knowledge, powers and instructions for taking action upon the receipt of the disclosure from a RE. Ensure that all REs are made aware of information on reporting form, contact point and reporting channels, including that this information is publicly available.

c) Ensure immediate communication of the designations and further amendments in the PF–related UN TFS to the REs.

d) Ensure more frequent coverage of implementation of TFS obligations in supervisory inspection, focused on the weaker performing sectors and provide with the necessary resources. Ensure that the TA develops UN TFS inspection procedures and trains the staff to implement them.

e) Provide clear guidance to REs, especially to DNFBPs, on their obligations under PF–related UNSCRs for freezing, unfreezing, reporting (included attempted transactions). Conduct further outreach to REs on their obligations.

## 4.2. Immediate Outcome 9 (TF investigation and prosecution)

327. Croatia's legal framework to fight TF is in line with international standards to a large extent. However, some deficiencies have been identified (see R.5). The main CFT bodies in Croatia are: (i) the SIA authorised to detect and understand security threats and challenges by collecting and analysing intelligence significant for national security, including terrorism and TF; (ii) the Counterterrorism Department (CTD) within the PNUSKOK, which monitors the situation of terrorism, international terrorism and other related crimes and events and is directly involved in investigations of terrorism–related crimes; (iii) County SAO in charge of formal criminal investigations of the TF cases, as well as overseeing the work of the LEAs in detecting crime.

### *4.2.1. Prosecution/conviction of types of TF activity consistent with the country's risk–profile*

328. There has been no TF prosecution or conviction in Croatia so far. However, given the deficiencies identified in the risk assessments, the assessment team cannot reach the firm conclusion that this is in line with the risk profile of the country. Details on the understanding of risk are further elaborated.

329. The ALMO conducted some TF–related activities, including analysis of concrete TF cases and its dissemination to authorities (mainly the SIA), as referred to under IO.6.

330. The SIA stated that they compile TF risk analysis (confidential classification) with the aim to prevent illegal activities. They carry out trainings on TF techniques, to enhance knowledge of new typologies such as "virtual currencies/transactions and new risks". The SIA indicated that for this purpose, they collect qualitative and quantitative information, analyse TF threats and vulnerabilities and evaluate the TF risk in order to identify CFT priorities, considering the regional and global context. However, particularities of their analysis were hardly described to the assessment team and mainly presented in general terms. In addition, very limited documents have been provided which would support their arguments.

331. On the other hand, Croatia has incorporated very limited analysis of the TF risk in the NRA (see also IO 1). The 2016 NRA identified a medium–low TF risk[140], but the 2020 NRA estimated the TF risk as low[141]. No consistent explanation was provided for this change in the level of TF risk. On–site, authorities have regularly referred to that in Croatia there is no terrorism and therefore no TF risk. After the on–site, Croatian authorities stated that this reduction of the level of TF risk is due to the closure of the so called "Balkan route" in March 2016, the end of the migrant crisis (from 2015–2016), and the improvement of the legal framework. However, none of these differences was explained in the 2020 NRA. In addition, the 2016 NRA was approved in December 2016 and, thus, some of these circumstances would have been already captured there. The 2016 NRA Action Plan also did not include any measure specifically related to the mitigation of the TF risk (only general measures concerning TF were included). Furthermore, the 2020 NRA still refers to migrant crisis associated risks and the so–called "Balkan route" and do not mention its closure as an influence on the reduction of the threat to TF. However, its action plan does not contain any particular measure concerning TF (only general measures concerning training and strengthening of the different AML/CFT bodies are included). Consequently, the assessment team still believes that TF risk is not fully analysed and understood and the reduction of the TF risk in the 2020 NRA has not been explained nor supported by objective data.

332. In terms of national TF vulnerabilities in the NRA, it was noted that the assessment is based on the analysis of the following variables: political environment, normative regulation of terrorism/counter terrorism, the criminal offence of TF, co–operation of competent authorities, analysis of suspicious transactions, adequacy of resources, international co–operation, international restrictive measures, non–profit organisations sector, cash transfer across the state border, and money remittance services. However, none of these variables has been sufficiently analysed and assessed to determine the potential level of TF vulnerabilities. On the contrary, reference was only made to the legal and institutional framework, as well as general statistics

[140] Page 14 of 2016 NRA.
[141] Page 245 – 268 of 2020 NRA.

without any substantial and valuable conclusion. The following analysis is missing, as described below.

333. Administrative capacities in terms of identification and investigation of the TF have been mentioned in the NRA, but only to a limited extent. While some recruitments have been carried out in the AMLO based on the outcomes of the NRA, the still existing lack of adequate human resources in the AMLO has not been assessed as to how it impacts TF identification. Additionally, there is a lack of financial investigators within the SAO which was not indicated in the NRA, nor has the impact of this deficiency on the potential TF investigations been determined.

334. The 2020 NRA identifies that ISIL has used migration routes to inject members into the European territory[142], but authorities showed no in–depth understanding of this phenomenon, neither detailed analysis was shown to the assessment team to assess potential areas of risk. Even though the SIA indicated that they look at all information regarding possible TF financial flows related to the above–mentioned risk, this seems to be inadequate since TF can be committed by providing any kind of funds, not necessarily financial. Therefore, there is no full understanding by the authorities of how the limited value of different kinds of funds carried out by migrants can be used for TF purposes.

335. Furthermore, besides the fact that a certain NPO has been carrying out projects regarding migrants, there is no comprehensive analysis conducted and understanding demonstrated of the potential ways that those activities can be abused for the TF purposes. The SIA briefly described a case from 2015 when radical ("*salafi*") individuals were prevented from establishing an NPO whose "cultural" activities would be used as a cover for financing extremist activities, including possible TF. However, no details on particular actions were described to the assessment team, especially in terms of whether those activities were investigated in order to establish a potential TF offence. The SIA also stated that information regarding activities on NPO is regularly analysed, but these analyses were not provided or the conclusions summarised to the assessment team.

336. Croatia recognises itself as a transit country used by organised criminal groups. However, there is no risk assessment of the potential link between OCG and TF conducted, nor have authorities shown an in–depth understanding of the potential problem. Even though the SIA pointed out that they collect intelligence on the activities of OCG and that, to date, no links between OCG and TF have been established, the assessment team was not provided with the details of the analysis. Even the general findings of the analysis have not been presented, and therefore the assessment team cannot make any conclusion whether their understanding is in line with the risk profile of the country.

337. One of the risks that authorities have highlighted is the remaining stock of weapons in Croatia. It was considered in the framework of the national counterterrorism strategy. Nonetheless, the assessment team was not presented with the understanding or analysis of the potential risk to TF (it is not sufficiently analysed in the TF–related section of the NRA). This is especially relevant considering that different kinds of funds can be used to finance terrorism (including weapons or event elements of it). Croatian authorities affirmed that, in most cases, weapons were found in possession of war veterans and investigations that were carried out in such cases ruled out all links to potential TF or "*terrorist ideology*", but the exact number of such

[142] 2020 NRA p. 245

cases and related investigations were not shared with the assessment team. In addition, some cases of the smuggling of weapons have been presented to the assessment team.

**Box N°4.1: Smuggling of weapons case**

In 2018, the USKOK conducted a criminal investigation in co–operation with Germany and Switzerland, which revealed that OCG operating in Croatia from 2016 to 2018 smuggled several pieces of firearms, ammunition, and explosives from Croatia to Germany as a destination country. Evidence and data collected during the investigation were exchanged with EUROPOL and Germany. Based on the information received by German prosecutors, a search warrant was issued in Croatia for the search of homes and other premises of German nationals, who were linked to the extreme right organisations in Germany and who were acquiring firearms from the Croatian OCG. During the international criminal investigation against the OCG members in Croatia, financial inquiries were conducted that revealed no elements of terrorism financing. The investigation resulted in the arrest of several individuals and weapons and other items were seized. USKOK prosecuted all the arrested persons who were later convicted only for the smuggling of weapons offence.

Although a formal TF investigation was not launched, Croatian authorities affirmed that potential TF implications were considered. In particular, financial inquiries were conducted to determine if funds were transferred to conflict areas or terrorism–related persons, but no link with TF was established. Several authorities were involved in this case (the Police, the USKOK, the SIA, etc.) While Croatian authorities were aware that the provisions of weapons for terrorist purposes could be qualified as TF, the investigation was solely focused on financial flows.

338. FTFs have been generally mentioned in the NRA. The authorities identified seven Croatian nationals residing in the territory under ISIL control. The NRA states that none of them was radicalised in Croatia. One of them was identified as having solely Croatian citizenship, while the other had dual citizenship. Authorities acknowledged that some of the family members of these FTFs were sending small amounts of money, however, they have not considered this as TF, explaining this by the fact that the volume of funds under consideration would hardly support the terrorist activity (see Core Issue 9.2). Although the SIA indicated that FTFs related to Croatia in conflict areas were detected, and they looked into their financial backgrounds, transactions and links to other entities, in the context of possible TF, the MFEA referred that there has been no substantial evidence acquired so far that would help to clarify the nature of these persons stay and behaviour and to assess whether or not they have been involved in terrorist activities or (un)willingly came to Syria/Iraq as members of families of terrorists. Furthermore, the NRA states that returning of the foreign fighters represent a major risk to the European society in the context of TF, but it was unclear how Croatia is not affected by this phenomenon since they are an EU Member State. Neither the NRA nor the authorities could demonstrate that they have a clear understanding of this problem.

339. There has been no separate analysis of the vulnerabilities of certain sectors regarding TF reflected in the NRA. The assessment does not make a distinction between the specific ML and TF vulnerabilities in FI and DNFBP sectors. Even though the majority of TF STRs are coming from the REs, no in–depth reasons were provided to the assessment team as to how specific sectors and products are potentially vulnerable.

340. While there have been STRs submitted to the AMLO by REs, as well as submissions from the foreign FIUs and subsequent dissemination (45 out of 51 cases have been disseminated to the SIA and only 6 to the LEA[143]) no analysis was conducted on typologies used and the reasons for no further investigation of cases. The NRA does not contain detailed analysis of the reasons for the lack of STR reporting by various sectors.

**Table 4.1: Annual FIU statistics on the TF cases**

| Year | Reporting entities[144] | State authorities [145] | Foreign FIU | Total no | Analytically processed | Cases disseminated |
|---|---|---|---|---|---|---|
| **2015** | 7 | 1 | 5 | 13 | 12 | 10 |
| **2016** | 5 | 2 | 6 | 13 | 10 | 12 |
| **2017** | 4 | 4 | 4 | 14 | 15 | 11 |
| **2018** | 5 | 2 | 2 | 9 | 8 | 6 |
| **2019** | 14 | – | 2 | 16 | 10 | 7 |
| **2020** | 12 | – | – | 12 | 3 | 5 |
| **total** | 47 | 9 | 19 | 77 | 58 | 51 |

341. Some case examples related to TF suspicions were provided to the assessment team. While some cases described how the AMLO used its powers to analyse and disseminate the case, further information concerning actions taken during the pre–investigative stage was not presented or was presented to the team in general terms, simply stating that TF elements were not confirmed and, thus formal investigation was not launched.

**Box N°4.2: MO case**

The AMLO started operational analysis of transactions and persons based on a notification from a legal entity providing money transfer services through an MVTS. According to the provided data, natural person X received funds once a month, stating that the receipts represented an aid for the celebration of Ramadan. This person was also registered as a sender of money and explained that it was for the purpose of helping other people. X tried to withdraw the funds sent to him twice, but due to some errors in X's name and surname, the funds could not be withdrawn, suspecting the RE that those errors were not accidental. The same person X was also linked to other natural persons who avoided answering additional questions or cited that the purpose of a transaction was financial assistance for the costs of celebrating religious holidays.

The AMLO determined that the senders of the money in favour to X were various natural persons, most often from France, Germany, Belgium and Italy. Likewise, in the case of their natural persons linked to X, it was determined that they received funds from various natural persons from many third European countries and the USA. The checks in the police databases showed that in 2016 X was registered for the criminal offence of illicit possession, manufacture, acquisition of weapons, being convicted for this crime.

Based on the referred analysis, the AMLO decided to disseminate this case to the SIA, which does not have law enforcement powers. Although the concrete actions undertaken were not indicated, Croatian authorities informed that the SIA carried out an operational investigation

[143] Additional analysis and comments related to the effectiveness of the AMLO, p. 30.
[144] Number of STRs submitted by REs.
[145] Number of cases submitted by competent state authorities to the AMLO.

including informal international co–operation. Based on these actions, the case was finally closed, and a formal investigation was not launched. According to the information gathered on–site, the prosecutor did not intervene in this case.

342. Croatian authorities indicated that upon receiving information that a person may be linked to terrorism or TF, the Police, together with the SIA, conduct inquiries. They check domestic and international databases, telephone numbers used, border crossing records and exchange information with Europol and Interpol. The information is also obtained from competent authorities such as the AMLO and the TA. None of these resulted in confirmed suspicion of TF. These findings are gathered and stored as intelligence.

343. In the view of the assessment team, the lack of criminal investigations is partly caused by the overreliance on the information gathered by an intelligence agency (which is not an investigative body). It is also partly caused by the lack of comprehensive understanding of the nature of TF, as well as the ways how certain sectors can be abused for TF purposes.

344. In addition, Croatian authorities appeared to have a lack of understanding as to how foreign TF threats may have TF implications in Croatia given the close cultural, social, economic and historical links between Croatia and some of their neighbouring jurisdictions.

### *4.2.2. TF identification and investigation*

345. There have been no TF investigations nor a proactive approach concerning TF identification was demonstrated. Croatian authorities did not show a full understanding of the TF phenomenon.

346. The authorities have detected some potential cases of TF, and only preliminary inquiries have been undertaken concerning TF. Several notifications containing intelligence on TF were disseminated by the AMLO to the SIA and the CTD. Dissemination of the cases to the SIA can cause certain problems as the SIA do not have law enforcement powers (see IO.6). However, the assessment team was not presented with clear arguments as to why particular actions taken with respect to these disseminations were not related to TF offences (see also Core Issue 9.1).

**Box N°4.3: TF inquiry**

In 2015, based on initial information of the SIA, the police conducted inquiries on suspicion of TF related to a purchase of a large area of land (both agricultural and construction land) in Croatia by Croatian companies, which had been founded and legally represented by foreign nationals of high–risk countries in terms of TF. The land is situated near the Croatian border with a neighbouring country, more precisely, villages and towns in the neighbouring country identified as locations of interest to members of the Wahhabi movement. The intention was to build religious and residential buildings for members of the community.

In order to establish the source and purpose of the money transactions regarding the purchase of that land in Croatia, the police performed inquiries in co–operation with the SIA, the AMLO and the TA. The Departments involved in the inquiries within the Criminal Police Directorate were CTD, Economic Crime and Corruption, and Criminal Intelligence.

The inquiries conducted proved that no financial transactions were linked with TF. The SAO was informed thereof.

347. Particular actions taken by the authorities concerning the financial implications of potential TF related cases remain unclear. For example, the AMLO detected a case where a person convicted for arms trafficking was using the MVTS to transfer and receive money to/from other countries in a suspicious manner and informed the SIA, but no particular investigative actions were undertaken by the LEA in order to determine potential TF offence. In another case, in 2017, the SIA forwarded to the MoI and the SAO some information concerning a potential TF case, but further actions taken, if any, remain unclear.

348. Another possible source of information concerning TF would be international co–operation and MLA requests. According to the information provided, Croatia has established good international relations, especially with the EU Member States, to exchange TF and terrorism–related information and intelligence. During the assessed period, several international co–operation actions have been undertaken concerning terrorism and TF. According to the authorities, in some cases the requested states are reluctant to provide information, especially when they are requested through MLA/EIO. The SIA indicated that none of the information ever triggered any investigation of the TF offence in Croatia because concrete links with Croatia were not established.

**Box N°4.4: Information from foreign authorities as a source to initiate inquiries**

In 2020, a passenger car with the Czech license plates was checked at the Border Crossing Point of Stara Gradiška, entering Croatia from Bosnia and Herzegovina. The driver was a national of BiH. On this occasion, the check revealed several AK 47 automatic rifles. The criminal investigation revealed that the weapons were ordered by an unidentified person in Germany. The BiH national was using a cell phone with a Dutch call code. All data collected were sent through the SIENA channel to Europol for their information and analysis, as well as to Germany, the Czech Republic and the Netherlands for them to run the checks in their respective databases and supply any relevant information to Croatia on the person having been linked with criminal activities (including terrorism and terrorism financing). The requested countries replied that the person had no connections to terrorism but only to organised crime.

Croatia also received information from EUROPOL stating that no links were found between the case and terrorism or terrorism financing. A search of the phone of the suspected person was also undertaken, but no links to TF were found. Finally, it was only prosecuted for smuggling of weapons.

349. While there have been some MLA incoming requests related to terrorism or TF, this was not used as a potential source to detect TF activity in Croatia. In addition, there were no outgoing requests made by Croatia to foreign counterparts in relation to terrorism or TF suspicion, even though authorities indicated that the majority of cases had been linked with foreign countries.

**Table 4.2: Terrorism and TF related incoming international co–operation (Source: SAO[146])**

| Year | Offence | Incoming | | |
|---|---|---|---|---|
| | | MLA[147] | EIO[148] | EAW[149] |
| **2015** | **Terrorism/TF** | – | – | – |
| **2016** | **Terrorism** | 1 | – | – |
| | **TF** | – | – | – |
| **2017** | **Terrorism** | 2 | – | – |
| | **TF** | – | – | – |
| **2018** | **Terrorism** | – | 1 | – |
| | **TF** | – | 1 | 2 |
| **2019** | **Terrorism** | – | 1 | 1 |
| | **TF** | – | – | – |
| **2020** | **Terrorism** | 2 | – | – |
| | **TF** | 2 | 1 | – |

350. Authorities presented some FTF cases. It was obvious that authorities are not aware that even a small sum of money sent to the FTF family members can be a signal to further explore TF offence. Despite the links found between Croatia and the FTF, in the view of the assessment team, Croatian authorities underestimate Croatia's risk for the TF. In addition, the financial and non–financial implications of FTF cases were not thoroughly analysed by Croatian authorities. The SIA referred to cases of relatives of persons located in ISIL–controlled areas sending money to their relatives but, these cases have not been investigated as potential TF cases. The SIA informed that they checked all circumstances of these persons, and some financial aspects of these cases in the framework of the pre–inquiry investigation. Some authorities do not fully understand the different roles played by terrorist financers and how they can exploit different legal and illegal activities.

**Box N°4.5: Croatian FTF**

According to the information provided by Croatian authorities[150], a total of 7 persons with Croatian citizenship resided in the ISIL–controlled area. Of these, only one person has exclusively Croatian citizenship, while the others are dual citizens and have never lived permanently in Croatia. None of them has been radicalised in Croatia, nor have they joined ISIL from Croatia. According to available unconfirmed data, two men were killed in the fighting of the side of ISIL, while some women were in civilian camps under the control of the Kurdish–Arab SDF forces in Syria. Women generally joint ISIL as an escort of their "jihadist" husbands. At the time of the 2020 NRA there were six persons in the ISIL–controlled area, as one of the seven mentioned persons has returned to their country of origin in Western Europe.

351. While some terrorist attacks in central Europe have been allegedly committed with weapons coming from the Balkan area, Croatian authorities claimed that these weapons were not obtained in Croatia nor transited through its territory. While making only general statements, the authorities did not provide in–depth information to what extent they have analysed whether the weapons were coming from Croatia or not. According to the SIA, all cases of smuggling of weapons in Croatia are monitored, and the SIA did not identify any links to possible TF since, in general

[146] It is not consistent with the statistics provided by the Ministry of Justice.
[147] Mutual legal assistance.
[148] European investigation orders.
[149] European arrest warrant.
[150] NRA 2020, p.247

terms, smuggling of weapons in Croatia is related to people trying to get a fast profit in a small scale and not linked to TF or OCG.

**Box N°4.6: St. Mark's Square attack of October 2020**

In October 2020, a person started shooting with a weapon left from the Homeland War on St. Mark's Square (close to the Banski dvori), wounding a police officer in the process. The perpetrator ran off and killed himself afterwards.

According to the SIA, initial information after the attack, given that it targeted a police officer on guard duty in front of the building of the Croatian government, indicated that the attacker might be a member/follower of an extreme violent ideology. The investigation took several months, including expert examinations, searches of all property concerned, EIO, etc. According to the SIA, in order to clarify all circumstances of the attack, the source of the firearms used and any connection to other entities, a complete investigation of this person's financial background was carried out, including past and present financial transactions.

In this case, police conducted financial inquiries, taking the following main measures: (i) information on bank accounts of the attacker such as whether they are active or closed, balance of the accounts, when the last payments were made and who to and/or from; when closed, when and why the account was closed; the list of all account transactions for the period of three years back, (ii) information on the perpetrator's possible loans (when they were raised, the loan documentation, whether they have been paid out, whether there have been any debts, and if yes, what the loan debts were). All the information collected from banks and other financial institutions were analysed and submitted to the County SAO in Zagreb. The investigation concluded that the attack was due to a momentary mental state, and no links were found between the perpetrator and TF.

352. In addition, authorities did not demonstrate that they have undertaken appropriate steps to properly detect TF even though the evaluators came across several examples where potential TF activities should have been at least considered for investigation.

### *4.2.3. TF investigation integrated with –and supportive of– national strategies*

353. Croatia did not demonstrate to follow a general national strategy to deal with TF, rather, it is focused on case–by–case actions.

354. The 2015 National Strategy for the Prevention and Suppression of Terrorism has been adopted and serves as a key strategic document in the area of counterterrorism. This strategy is based on five pillars, and one is dedicated to TF measure of suppressing and disabling terrorist financing, fund collecting or aiding and abetting in any way terrorist organisations or persons linked with terrorism. This Strategy does not reflect specific and comprehensive actions concerning TF. The National Strategy for the Prevention and Suppression of Terrorism provides a general framework of counterterrorism action, which is made operational by the Action Plan.

355. An Action Plan for the Prevention and Suppression of Terrorism was also adopted to operationalise measures set out in the National Strategy and create an effective operational system for the prevention and suppression of terrorism, such as interagency coordination and international co–operation. The Action Plan refers to seven measures mainly focused on terrorism (preventive and repressive measures). Those measures mainly include (i) obligation to analyse and process intelligence and monitoring suspicious transactions, (ii) verification of

natural and legal persons related to restrictive measures, (iii) supervision of taxpayers and NPOs in accordance with TF risks, (iv) implementation of guidelines and risk assessment concerning ML and TF for some FIs, (v) protection against terrorist acts, (vi) reparation of damage and recovery from a terrorist attack, (vii) counterterrorism education and training and interagency coordination and international co–operation. While Croatia indicated that TF issues would be covered since the term terrorism also covers TF matters, specific measures directly related to TF mitigation of risk were not presented. Authorities informed that a new Action Plan is being prepared.

356. In 2014 Croatia established a National Committee for the Prevention and Suppression of Terrorism. Its main tasks seem to be focused on terrorism at the general policy level. Members and representatives of several Ministries and national bodies, including the SAO, the SIA, the AMLO and the Police, are represented in this Committee. Operational counter–terrorism coordination is conducted through the mechanism of the General Police Directorate's Operational Coordination and the SIA for terrorism and extremism issues. Authorities indicated that they exchange data and joint operations in the area of prevention and suppression of terrorism, extremism and radicalisation. However, while suggesting having a number of meetings, no conclusion, minutes or information on the outcomes of these meetings were shared with the assessment team to demonstrate that this Committee is operational.

#### *4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions*

357. In the absence of any convictions of TF, it is not possible to assess whether the criminal sanctions applied, in practice, are effective, proportionate and dissuasive. Sanctions envisaged in CC do, however, appear to be proportionate and dissuasive.

#### *4.2.5. Alternative measures used where TF conviction is not possible (e.g., disruption)*

358. No criminal justice, regulatory or other measures to disrupt TF have so far been employed when a TF conviction could not be secured. The authorities have, however, indicated that full co–operation and information exchange are provided to foreign countries when needed (see IO.2).

*Overall conclusions on IO.9*

359. In Croatia there is a National Strategy for the Prevention and Suppression of Terrorism, but this Strategy does not reflect specific and comprehensive actions concerning TF, nor is TF fully integrated into the counter–terrorism strategy.

360. Croatia's legal framework to fight TF is in line with international standards to a large extent. Although some elements to trigger TF investigations could have been further explored, there have been no investigations, prosecutions and convictions for TF offences. The AT came across several potential TF cases. A more proactive approach to TF would be needed, particularly where potential links of TF or FTF with Croatia may exist. Some authorities do not fully understand the different roles played by terrorist financiers and how they can exploit different legal and illegal activities. Hence, from the information provided, the evaluators concluded that major improvements are necessary.

361. **Croatia is rated as having a Moderate level of effectiveness for IO.9.**

## 4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

### *4.3.1. Implementation of targeted financial sanctions for TF without delay*

362. Croatia, as an EU Member State, applies the EU Regulations as a mechanism for the implementation of TF–related TFS under UNSCRs. At the national level, Croatia does not have additional mechanisms and procedures to remedy the deficiencies of the EU framework. Therefore, implementation of TFS for TF pursuant to UNSCRs 1267/1989 and 1998 "without delay" remains an impediment to Croatia's effectiveness. In addition, the national legal framework governing implementation of TFS for TF, including measures under UNSCR 1373, is still not in line with the FATF Standards. This has a certain impact on the effectiveness as described below.

**Table 4.3: Transposition of TF – related UNSCRs into EU framework in 2020**

| Date | Measure | Regime | Date of transposition into EU legal framework |
|---|---|---|---|
| 04.02.2020 SC/14097 | Designation | ISIL (Da'esh) and Al–Qaida | 11 February 2020 |
| 18.02.2020 SC/14113 | Amendment | ISIL (Da'esh) and Al–Qaida | 25 February 2020 |
| 23.02.2020 SC/14118 | Designation | ISIL (Da'esh) and Al–Qaida | 28 February 2020 |
| 04.03.2020 SC/14136 | Designation | ISIL (Da'esh) and Al–Qaida | 10 March 2020 |
| 24.03.2020 SC/14146 | Amendment | ISIL (Da'esh) and Al–Qaida | 1 April 2020 |
| 21.05.2020 SC/14195 | Designation | ISIL (Da'esh) and Al–Qaida | 26 May 2020 |
| 16.07.2020 SC/14256 | Amendment | ISIL (Da'esh) and Al–Qaida | 22 July 2020 |
| 10.09.2020 SC/14299 | Amendment | ISIL (Da'esh) and Al–Qaida | 17 September 2020 |
| 08.10.2020 SC/14321 | Designation | ISIL (Da'esh) and Al–Qaida | 13 October 2020 |

363. The Standing Group is the body responsible for the Introduction and Monitoring of the Implementation of International Restrictive Measures. The activities of the Standing Group are mainly focused on implementation of the EU sanctions, as it is not vested with explicit powers for implementation of the UN sanctions regimes. Formally, the Standing Group consists of 10 competent authorities[151] headed by the MFEA. It can also include other competent authorities of Croatia, when necessary. The Standing Group held its last meeting in 2019 (first half), where the members discussed amendments to the IRM Law to implement the FATF Standards. The country suggested that the Standing Group should meet on a quarterly basis, but due to the pandemic, no further meetings were arranged. Given the limited documentation and information, the assessment team could not assess whether the Standing Group meetings include discussions and

[151] Ministry of Foreign and European Affairs, Ministry of Defence, Ministry of Interior, Ministry of Justice and Administration, Ministry of Finance, Ministry of Economy and Sustainable Development, Ministry of the Sea, Transport and Infrastructure, State Attorney's Office, Croatian National Bank

decisions on implementation of the TF–related TFS measures under the UNSCRs and what are the roles and responsibilities of the members of this Group.

364. So far, Croatia has not identified individuals or entities or proposed any designations to the UN Security Council Committees pursuant to UNSCR 1267/1989 and 1988, as well as has not initiated designation pursuant to UNSCR 1373 at the domestic level and at an EU level.

365. The members of the Standing Group could not demonstrate a proper understanding and ability to take actions within the context of UNSCRs designations. There was inconsistency among members' understanding about their powers of proposing or making a designation under UNSCRs. This has also been affected by the difficulty of drawing distinction between UNSCR 1267/1989 and 1988 and UNSCR 1373. Authorities mentioned that since there are no terrorism and/or terrorism financing cases in Croatia, there is no necessity to have such a procedure in place. However, if the MoI, the AMLO, and the SAO have any intelligence on the potential terrorists or terrorist threat in Croatia, they will propose a designation. The assessment team considers that these do not demonstrate effective implementation of measures under UNSCRs designations mechanism.

366. Croatia did not demonstrate having adequate mechanisms and clear procedures in place to deal with the receipt of the direct requests from foreign states pursuant to UNSCR 1373. So far, Croatia has not received a request from a foreign jurisdiction for designation pursuant to UNSCR 1373. The authorities suggested that there is no need for setting separate mechanisms or procedures, should the case arise, diplomatic channels will be used for communication with foreign counterparts.

367. The website of the MFEA is the main platform for communication of matters related to TFS implementation. This contains a link to UN TF designation lists directing the user to: (i) the general page of the UNSC and not to the consolidated version of sanctions lists, and (ii) to the EU list and the interactive map of countries under UN and EU sanction regime. This measure, however, does not constitute immediate communication of the additions and amendments to the UN sanction lists of designated persons and entities to the REs. This has an impact on the implementation of the relevant UNSCRs by the REs that do not rely on automated sanctions updating and screening mechanisms, and had not subscribed to the UNSCRs newsletter on their own initiative.

368. In 2011 the Croatian Government passed a decision on setting up a Database on International Restrictive Measures, natural and legal persons and other entities to which the EU and UN restrictive measures apply. It was not, however, demonstrated that such a Database is established, in practice, and that it is operational. The authorities provided ambiguous responses about the existence, content and accessibility of this Database. In addition, neither authorities nor REs did ever refer to the Database when describing the source of information on the UN Sanction Lists.

369. Banks and other REs that are members of larger financial groups had sufficient understanding of UN TFS requirements. Among other REs, the Exchange services, E–money institutions, DPMS, Accountants, and Casinos displayed limited understanding of the need to verify information against the UN TFS when dealing with the Croatian or EU–Member States' nationals or legal entities.

370. Most REs demonstrated understanding of asset freezing requirements. Nevertheless, the understanding of the scope of these obligations varies among sectors. Some smaller FIs (Payment Institutions and Exchange services), DNFBPs (notaries, casinos, and real estate) and VASPs were

aware of the obligation to suspend a transaction and report to the competent authority when there is a match with a "sanction list". However, there was a mixed understanding as to the substance of "sanctions lists" where UN TFS lists were mentioned in conjunction with the EU, US, OFAC and FATF restrictive measures. The other REs have a perception that a minimum of 80% of information should match before the funds can be frozen, and the report filed.

371. Banks, MVTS and VASPs use sophisticated tools and supporting technologies that ensures a prompt update of the TFS sanctions lists and identification of the designated persons or entities. The customer databases are screened against the lists regularly (overnight). This includes automated analysis of the customers, BOs and other related natural and legal persons.

372. Some FIs (credit union, payment institution, authorised exchanges) and DNFBPs (notaries, lawyers, DPMS, casino, real estate brokers, and accountants) advised to mostly rely on manual checks. Among these, some mentioned subscribing to the UN TFS newsletter, and automatically receiving information of the updates to the UN sanction lists, thus ensuring timely access to this data.

373. Authorised exchanges, payment institutions, lawyers, accountants, casinos, notaries, and real estate agents demonstrated use of less comprehensive TFS controls. They have suggested that they would check the customers against the lists when the transaction is conducted. Otherwise, the frequency of screening would be determined on the basis of the customer's risk level and vary from once a week to every two years. Lawyers and Accountants advised that they would–check the customers against the lists also when changes in the customer profile (including change in ownership structure) would occur. Hence, these FIs and DNFBPs demonstrated that they would not identify a potential match of existing customers with the UNSCR sanction lists in a timely manner. Overall, the ability of the REs to detect a BO can impact detection of potential matches with UN TFS. While some banks demonstrated ability to identify not only the customers, but also their BOs (including when dealing with legal person that has complex ownership structure) and all parties of the transaction, other FIs could not confirm so. Among the non–bank FIs and DNFBPs, reliance on the newly established Croatian BO Register, the accuracy of which is yet to be tested (see IO.5), was observed.

374. In addition, the AMLO advised that it does not verify information on subjects involved in the CTRs and STRs against the UN sanction lists.

375. The outreach is conducted in the framework of the Annual Conference organised by the AMLO in co–operation with the Croatian Chamber of Commerce. Since 2012, REs are not provided with sufficient written guidance on their obligation in taking action under the UNSCRs sanction regime.

### *4.3.2. Targeted approach, outreach and oversight of at–risk non–profit organisations*

376. The NPO sector was considered within the scope of the two NRAs conducted in 2016 (subject to ML vulnerabilities in the sector) and 2020 (as a variable for assessment of the Country's TF vulnerabilities). In addition, Financial Inspectorate conducted a thematic analysis of business operations of foreign foundations and associations operating in Croatia in 2019 for the purpose of ML and TF risk assessment. None of these exercises led to identification of the subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse by virtue of their characteristics. The NPOs demonstrated no awareness that they could be abused for TF

purposes. The REs suggested considering NPO activities as a high–risk factor when assessing the risk profile of the customers.

377. In the 2016 NRA, the NPO sector was assessed against the ML vulnerabilities and scored at the medium level[152]. The analysis included reflection on the legislative requirements for registration of NPOs; and statistics on: (i) number of registered NPOs by types; (ii) number of submitted financial statements; and (iii) total annual turnover of NPO sector in 2012 and 2013. The identified vulnerabilities were related to lack of sanctions for violation of registration requirements[153], by inactive NPOs due to the complex process of liquidation and deletion of associations from the Register of Associations, as well as vague provisions on supervision[154], and the exchange of information amongst supervisors of NPOs[155]. The report also reflected on the mitigation measures, such as a requirement to conduct transactions above HRK 75 000 (EUR 10 000) through a bank account, and to ensure transparency of NPOs (keep information on purpose, goals of activities and membership), but did not analyse the effect of these, in practice.

378. The report on implementation of the 2016 NRA contains the following analysis on the domestic NPOs: "NPOs that are obliged to keep double–entry bookkeeping generated revenues from foreign governments and international organisations in the total amount of HRK 505 320 856 (EUR 67 376 114), while non–profit organisations that are obliged to keep simple bookkeeping generated revenues from foreign governments and international organisations in the total amount of HRK 4 188 890 (EUR 560 000). A significant part of the foreign funding was paid by foreign governments and organisations to NPOs established in the field of: protection of national minorities and sport activities (football clubs). Non–profit organisations that are obliged to keep double–entry books are on the date 31.12.2016. Disposed financial assets in a total value of HRK 16 268 503 368 (EUR 2 170 000 000). In 2016, non–profit organisations that are obliged to keep double–entry books had expenses in the total amount of HRK 411 547 867 (EUR 55 000 000) on the donation side (it is not possible to break down domestic from foreign donations)". This analysis raises questions as to what this aggregated data compilation can suggest in terms of the risks in the NPO sector, especially that it was even not possible to distinguish between the foreign and domestic donations, and also no analysis is conducted on the beneficiaries of the received funds.

379. In 2020, in the NRA, the NPO sector was analysed as one of the variables within the scope of assessment of the TF vulnerability in Croatia[156]. The NPO sector was not granted a rating for its TF vulnerability. The overall level of Croatia's TF vulnerability was assessed at the low level. As concerns the substance of the analysis, the NRA states that there was an important legislative change made to overcome the vulnerabilities identified in the 2016 NRA. This legislation regulates the system of financial operations, accounting and supervision of financial operations and accounting of NPOs. It sets a mandatory requirement for registration of the NPOs and

[152] NRA 2016, p. 180 "Taking into account the above Structural Risk Indicators and valuing them in an Excel model for vulnerability to ML assessment, the working group has rated this sector – M."
[153] NRA 2016, p.178 "some non–profit organizations have still not fulfilled this obligation since the obligation of registration in the register of non–profit organizations at the Ministry of Finance is not required by law but by the decree and thus the violation of this obligation has no sanctions."
[154] NRA 2016, p.179 "Also, the complex process of liquidation and deletion of associations from the Register of Associations, as well as vague provisions on supervision have led to a large discrepancy between the number of registered and really active associations."
[155] NRA 2016, p. 179 "Supervision of this NPO sector is dispersed among several bodies.", p. 182 "The exchange of information amongst supervisors of NPOs should be enhanced"
[156] NRA 2020, p. 252

introduces the obligation to submit financial statements[157]. In addition, the report reflects on the change in the status of associations, including statistics for 2015–2018 on: (i) total number of registered associations; (ii) number of associations that harmonised their statutes in accordance with the Associations Law; (iii) the number of "passive" associations (that had not held the assembly meetings for more than 8 years); (iv) the number of associations in the process of termination of operation, and the annual total of deleted ones[158]. This information in the NRA, however, represents factual data, focused exclusively on associations (and not also foundations), with no analysis of the impact of these legislative amendments on vulnerabilities in the NPO sector or the effect that the harmonisation or deletion of passive associations had on the TF vulnerability in the sector.

380. The thematic analysis on business operations of foreign foundations and associations operating in Croatia in 2019 conducted by the Financial Inspectorate concluded that the risk of abuse of foreign associations and foundations for ML and TF in Croatia is low[159]. Nevertheless, this document does not focus on the foreign foundations and associations in their capacity as an NPO. The analysis also does not make a distinction between factors that would contribute to potential ML risks for foreign foundations and associations and risks related to TF.

381. This document: describes the legislative framework for operating foreign foundations and associations in Croatia; lists data from the MoJA Register (title, registration number etc.); aggregates data contained in the "Revenue and Expenditure Statement"; and aggregates data on turnover.

382. On the basis of this entry data, the Financial Inspectorate established that: the headquarters of foreign associations and foundations are not in the high–risk jurisdictions[160]; goals of entities are legitimate; financial flows are adequate to the goals of entities ("no donations received from unknown donors or individuals, in small sums"; "the obtained funds used for staff salaries, material costs and donations to other related NPOs, also without links to red flag indicators (donations to natural persons/terrorists/terrorist organisations"); no operations conducted in cash, and all entities have bank accounts (although out of 151 only 32 foreign associations were analysed[161]); no negative media information observed; financial reports are filed in line with legislation; self–assessment questionnaires are filled in and filed; and no suspicion of exploiting a legitimate NPO is misused for ML or TF.

383. This document demonstrates the attempt of the authorities to assess the TF risks of the NPO sector but raises questions about the adequacy of information used and analysis conducted to support the conclusions. In particular, information coming from limited sources (with no proper consideration of NPO Register, supervisory data, STRs, intelligence and criminal data, and foreign co–operation information), and analysis having a narrow focus with no consideration of risks related to donor NPOs, and donations (directions and beneficiaries). Some conclusions are also questionable because they are not always in line with other information provided by the

[157] NRA 2020, p. 265
[158] NRA 2020, p.266
[159] Analysis of business operations of foreign associations and foundations in the Republic of Croatia in 2019 for the purpose of ML and TF risk assessment, p.8.
[160] EU Member States, USA, Japan, Serbia and Bosnia and Herzegovina.
[161] Analysis of business operations of foreign associations and foundations in the Republic of Croatia in 2019 for the purpose of ML and TF risk assessment, p.3. "At the end of 2019, 151 foreign associations were entered in the Register […] in 2019, 32 foreign associations (sample for Analysis) realised transactions through accounts opened in banks in the Republic of Croatia"

country in the course of the assessment, as described further below (e.g., on suspicion of exploiting a legitimate NPO, size of the turnover of foreign NPOs).

384. According to provided information, in Croatia, there are 42 782 registered NPOs. The large majority of NPOs are associations (see Chapter 1). The Register of NPOs is a central source of data on NPOs necessary to determine and monitor the obligation of preparing and submitting financial statements, their financial position and business operations and use of earmarked budgetary funds. Additional information is also available on the Registers of Associations and Foundations (see IO.5). These together ensure transparency of information about NPO's activities and good standing.

385. NPOs are registered in the Register of NPOs on the basis of the application submitted to the MoF not later than 60 days after the registration thereof in the principal register. The Register of NPOs does not monitor the quality and accuracy of information submitted by the registered NPO and checks only the completeness of submitted information. The Register does also not conduct criminal background checks and checks against UN TFS for NPO founders and members/volunteers. Fines can be applied against an NPO if it does not register itself in the Register of NPOs or inform of the changes in data entered into the Register. While 8 cases were identified over the period of 2015–2020, no practice of application of sanctions is demonstrated.

386. The Register of NPOs also contains data on inactive NPOs. This was explained by a preference of the NPOs to stay registered to retain the company history. From 2015 to January 18, 2020, the number of NPOs that submitted the statement on inactivity was 2901. No measures are taken to detect and monitor the inactive NPOs. While no practical examples were brought to the attention of the AT, in such circumstances, the vulnerability is that if it occurs, the TF abuse of the inactive NPO might not be detected timely. The authorities explained that the termination of the NPO is possible only by the latter's initiative, which is an obstacle. At the same time, facing the issue, the authorities expressed their willingness to improve the system to enable initiation of the dissolution process.

387. Registering in the Register of NPOs is a condition for obtaining the funds from the state budget, other public resources and EU funds. This is coordinated through the Office for Co–operation with NGOs. These funds are provided to NPOs by a banking transfer. In the period of 2015–2020, 4 breaches were identified where the responsible person of the local self–government unit allocated funds to NPOs that were not registered in the Register of NPOs. An indictment for a misdemeanour was filed against the responsible person of the local self–government unit, but not the NPOs. No further information on the sanctions applied, in practice, is available.

388. As described under R.8, all NPOs are subject to a number of transparency and reporting requirements. These, nevertheless, do not seem to include the ones that would require the NPOs to apply measures for ensuring the integrity of its own founders and members, ensuring the appropriateness of the source of the raised/collected funds, and ensuring that when implementing projects, risk of TF support is prevented.

389. Authorities informed that in 2020 the income of NPOs generated from public sources, donations of foreign governments and international organisations amounts to 38%. Other 62% of funds are comprised of donations made by: the membership (13%), companies and other legal entities (4%), citizens and households (2%), the sale of goods and services and rendering services (19%), as well as from revenues/receipts under special regulations (14%), other NPOs (3%) and

from other sources (7%). The percentage of sources of funds is almost the same for 2019. Overall, it can be observed that only a third of the NPOs income is formed from the low–risk sources.

390. Supervision of NPOs was introduced in 2015 and is carried out by the MoF, Department for Financial and Budgetary Supervision (DFBS), and the Financial Inspectorate related to the supervision of the foreign exchange operations of foreign associations and foundations. Supervision is not risk–based, and the supervisors are mainly focused on the tax compliance of NPOs. Although the supervisory authorities informed that they set annual inspection plans for the NPOs, which include the number of planned inspections of NPOs, this was not made available to the evaluation team for verification. The supervisors confirmed to lack the resources for supervision of NPOs which affects effective supervision.

391. The DFBS conducts complaint–based inspections. Priority for conducting supervision is given to requests that contain evidence of suspicion of a criminal offence, including from the SAO (19) and the MoI (the Criminal Police Department) (13); and requests containing information about the breach of legislative requirements, including from the State Treasury, Department for State Accounting and Accounting of NPOs (180), and other competent authorities (11), citizens (14), or submitted anonymously (18). Authorities suggested that these requests were mainly related to suspicion of illegally withheld property gain by members or responsible persons of the association and exceeding the position and authority of association; inaccurate bookkeeping; or non–submission of the annual financial reports. There were no complaints received related to TF abuse of an NPO.

392. Financial Inspectorate plans and conducts supervisions taking into account the amount of turnover of non–resident accounts of foreign NPOs, which are collected from commercial banks on an annual basis and the country of origin from which the founders of NPOs come.

**Table 4.4: Number of registered NPOs and turnover on non–resident accounts of NPOs in 2019**

| Description | Foreign associations | Foreign foundations |
|---|---|---|
| Number of registered NPOs | 151 | 12 |
| Number of NPOs active on non–resident account | 32 | 6 |
| Overall inflows to the non–resident accounts of NPOs in EUR | 11 427 513 | 650 008 |
| Overall outflows from the non–resident accounts of NPOs in EUR | 11 406 154 | 708 070 |

393. The supervisory bodies informed that supervision includes monitoring of the financial statements, lawful collection of funds from public and other resources, as well as ascertaining if the funds are used in line with the objective of the NPOs stated activities. Supervisory efforts are mainly focused on the control of the allocation of funds from public sources. No further information was given to the AT about the process of analysis of lawfulness of collection of funds. Overall, such supervisory focus on the use of the public funds in line with the objectives of the NPO, would not ensure detection of instances when: (i) funds from other sources provided to the NPOs are linked to TF, and (ii) the funds are made available to terrorist financiers directly or indirectly. Fundraising by the NPOs falls out of inspections' focus, including when linked to the financing of foreign projects and high–risk countries.

394. In the period of 2015–2020, the DFBS received 1 request for performing supervision of the foreign NPO, which, however, could not be carried out due to the unavailability of data for

surveillance. In the period of 2014–2019, 4 supervisions were conducted by Financial Inspectorate on foreign associations, the turnover of which had changed significantly during that period. On one occasion, the breach of foreign association detected by the Financial Inspectorate, was related to tax avoidance. While 364 financial inspections of domestic NPO were conducted over the period of 2015–2020, none of these revealed potential signs of TF. The authorities did not provide information on the nature of identified breaches, the types of NPOs, and the sanctions applied, in practices. Considering the type and size of sanctions envisaged under Financial Operations and Accounting of NPOs Law (FOA NPOs Law) that are limited to fines, of max EUR26 000, these are not deemed proportionate, dissuasive and effective.

395. Limited understanding of the TF risks displayed by the country potentially also affects application of appropriate measures, including gathering of information and conducting investigations for the detection of instances of possible abuse of NPO for TF purposes. This was evidenced by the statement of the authorities that in the circumstances when funds of the NPO are of a legitimate origin, the NPO cannot be potentially exposed to TF abuse. These explanations of the authorities raise doubts.

396. REs demonstrated uneven awareness of risks in the NPO sector, this being the reflection of the inappropriate analysis provided in the NRA. Some REs advised classifying NPOs as high–risk customers by default, but the others advised to apply a case–by–case approach and conducting own risk assessment in line with internal policies and procedures, thus demonstrating a positive practice.

397. The AMLO informed that in 2020 there were 18 STRs filed by REs (16 from banks and 2 from MVTSs). STRs concerned the transactions indicating economic activity that were performed on the association's account, the suspicions on misuse of NPO for fraudulent activities, as well as the suspicions on tax evasion. As a result, no links to the TF were identified by the AMLO.

398. The NPOs demonstrated no awareness that they could be abused for TF purposes. This is because there were no targeted outreach and educational programmes organised by the authorities to raise and deepen awareness among NPOs about the potential vulnerabilities of NPOs to TF abuse and TF risk and the measure that NPOs can take to protect themselves against such abuse. The NPOs are invited only to participate in the Annual Conference on the Prevention of ML and TF. So far, no awareness–raising activity has been undertaken for the donor community.

### *4.3.3. Deprivation of TF assets and instrumentalities*

399. Croatia has not frozen assets pursuant to the sanctions regime under UNSCR 1267/1989, 1988 or 1373. Hence, there was no practice of application of measures with respect to unfreezing of funds.

400. Most REs could describe steps they would take to implement their asset freezing obligations pursuant to respective UNSCRs. Banks, and Life Insurance Companies confirmed that the checks at the on–boarding stage and further customer monitoring sometimes reveal some partial matches. Further detailed examination determined these cases to be false positive matches.

401. All REs mentioned that in the event of a positive match, they would report it. Despite the MFEA being a designated authority for the receipt of freezing reports, many REs (including, but not limited to credit union, payment institutions, E–money providers, pension insurance

companies, lawyers, notaries, real estates, DPMS, and casinos) were not certain as to which authority to report to. The majority considered the AMLO (as also confirmed, in practice), and some also mentioned the MFEA and the MoI to be the competent authority. The evaluation team considers this is a result of a lack of: (i) established clear mechanism and channels for communication; (ii) reporting form for submitting such reports to the MFEA; and (iii) determined recipient of these disclosures (contact point). It was not evident for the AT whether the MFEA responsible department has clear instructions and knowledge for acting upon the receipt of a report.

402. Small FIs (Exchange offices, Payment Institutions, and E–money Institutions) and DNFBPs (real estates, lawyers, and accountants) stated that in case of a match with UN sanctions lists, they would simply refuse the transaction or exit the customer relationship with no further report filed. This does not prove to be an adequate and effective implementation of the TFS obligations and suggests that the listed persons and entities would be deprived of respective assets in these circumstances.

403. In the absence of the TF prosecution and conviction, there were no criminal freezing or confiscation orders made in relation to terrorists, terrorist organisations and terrorist financiers. No other measures to deprive terrorists of assets were applied.

### *4.3.4. Consistency of measures with overall TF risk profile*

404. Overall, TF risk understanding is insufficient among the authorities in Croatia. This respectively affects the adequacy of measures taken for implementation of the TF–related UN TFS and prevention of the abuse of NPOs for TF purposes.

405. The Standing Group did demonstrate no clear steps taken to implement TFS measures under the UNSRCs. Shortcomings related to communication of designations at the national level, and mechanisms in reporting to the designated authority, weakens the effectiveness of the TF–related TFS regime in Croatia.

406. Due to the lack of a comprehensive understanding of the TF risks pertaining to the NPO sector, as well as the identification of the sub–set of NPOs that may be vulnerable to TF abuse, Croatia does not appropriately apply focused and proportionate measures, including risk–based monitoring towards the NPOs sector. Croatia did not demonstrate conducting sustainable outreach to the NPOs sector and the donor community.

## *Overall conclusions on IO.10*

407. Croatia implements the UNSCRs with delay, as it has not set a national mechanism that would overcome the delay occurring at the EU level. Croatia does not have sufficient domestic mechanisms for identification and designation of persons and entities pursuant to UNSCRs 1267, 1988 and 1373. The Standing Group did not demonstrate actively performing its role in implementation of the UN TFS. No sufficient level of outreach and guidance is provided to REs.

408. Nevertheless, various measures applied by the REs themselves assist in reducing the impact of some of the mentioned deficiencies. Notably, the delay in implementation of the UNSCRs by the larger FIs that use commercial databases and the REs that are subscribed to the UN newsletters affects to a lesser extent, thus reducing the materiality of the issue. While no funds are frozen, the REs suggested detecting false–positive matches, thus demonstrating abilities to identify potential cases. The most material sectors of REs demonstrated the ability, knowledge and understanding of the implementation of their TFS obligations.

409. While Croatia took measures to understand the risks in the NPO sector, these did not prove successful. Weaknesses in assessment of NPOs risks affect application of risk–based efforts.

410. Limited understanding of the vulnerabilities of the NPO sector to TF abuse, deficiencies in the national framework of implementation of the TFS, including identification and designation of persons and entities, have a significant impact on the level of effectiveness of the Croatian TF–related sanctions regime.

411. **Croatia is rated as having a Low level of effectiveness for IO.10**

## 4.4. Immediate Outcome 11 (PF financial sanctions)

412. Croatia's economy includes industries and companies producing military, dual–use or nuclear–related items. Croatia has some nuclear power production and companies offering international trade and shipping services. The competent authorities, including the Commission for the Control of Dual–Use Items and the Commission on the Prevention of WMD, play an active role in monitoring the trade to ensure implementation of counter–proliferation measures.

413. Iran has an embassy in Croatia and diplomatic personnel. Croatia has trade relations with Iran, which is related to foodstuff, medicine, etc., in 2020 and amounted to approx. 0.032% of exports and 0.09% of imports of Croatia. The insignificant volume and nature of trade do not entail exposure of Croatia to evasion of PF–related UN sanctions.

414. Croatia informed that diplomatic relations with the Democratic People's Republic of Korea (DPRK) were established in 1992, but there is no embassy in Croatia and no diplomatic personnel[162] residing in the country. The country suggested no trade to occur between Croatia and the DPRK.

415. Croatia has no correspondent banking relationship established with both Iran and the DPRK.

### *4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay*

416. In Croatia, the mechanisms in place for the implementation of PF–related UN TFS are similar to those outlined in IO.10, related to the UN TFS regime for TF.

417. The implementation of targeted financial sanctions (TFS) for PF pursuant UNSCRs 1737(2006) and 1718(2006) in Croatia is based on the European legal framework. These regulations apply freezing measures to a broad range of funds and property. Freezing obligations under European regulations are applicable to all natural persons and all legal persons within the EU and take effect immediately on publication of the regulations in the EU's Official Journal. Implementation without delay, therefore, remains an impediment to Croatia's effectiveness. Croatia does not have additional national mechanisms and procedures to ensure timely implementation of the TFS on PF.

418. In practice, technical problems related to implementation of measures applied within the UNSCRs of DPRK, "without delay" under the EU framework, yet remain.

[162] http://www.mvep.hr/en/diplomatic–directory/diplomatic–missions–and–consular–offices–to–croatia/democratic–people%e2%80%99s–republic–of–korea–(the)–bucharest,290.html#p

419. As concerns mechanisms regarding Iran, the technical problems related to timely implementation of measures did not have a practical impact, since the list of individuals and entities is wider in the EU framework and at a time included already the respective UN designations.

420. In addition, there are additional mitigating measures applied by the EU requiring prior authorisation of transactions with designated Iranian entities. This allows the authorities to determine if the transfer of funds for which the authorisation is requested would be permissible according to the EU Regulations.

421. The Standing Group headed by the MFEA is also the body responsible for implementation of PF–related UN and EU sanctions regimes and monitoring of their implementation, but, as described below, it did not demonstrate performing actively its role in implementation of asset freezing requirements in the country (see IO.10).

### *4.4.2. Identification of assets and funds held by designated persons/entities and prohibitions*

422. There were no funds or assets identified, and frozen in Croatia pursuant to UN designations related to PF.

423. Most REs demonstrated awareness of asset freezing requirements. There were no real matches detected with the UN sanction lists on PF, but several REs confirmed to have had false–positive matches. This demonstrates vigilance of the private sector and the ability to detect designated persons and entities. As described in IO.10, there was nevertheless a mixed understanding as to the "sanctions lists" to follow. Overall, the ability of the REs to detect a BO can also potentially impact detection of funds or assets owned indirectly.

424. So far, there were also no investigations and prosecutions related to proliferation or PF conducted in Croatia. Authorities did not demonstrate to have an effective coordination mechanism in respect to combating PF. They mentioned that should the case arise, they would benefit from existing proliferation coordination national mechanisms, such as the Commission for the Control of Dual–Use Items and the Commission on the Prevention of WMD to support early identification of proliferation.

425. Croatia has developed a National Strategy for the non–proliferation of weapons of mass destruction aimed at ensuring improvement of coordination of the existing systems for suppression of WMD, strengthening the capacities for collection, exchange and analysis of intelligence data necessary to detect, identify and monitor threats caused by WMD and associated dual–use and military–use items. These measures, while indirectly, also ensure prevention of financing of proliferation of these goods.

426. In order to demonstrate the effectiveness of coordination among the competent authorities, the CA provided an example of an ongoing case on attempted export where a person declared to export certain mono technology driven to interfere mobile communication. The CA instructed the declarant to address to the competent authority to clarify whether the export of the object requires authorisation. The declarant refrained from exporting the object, explaining that the buyer had changed his mind. A few days later, the same person tried to export the same good by changing its description, which, however, was detected. While this part of the case does not reflect on the investigation into the financial aspect, this was done at a later stage, falling out of the evaluation scope. Hence, the authorities demonstrated the ability to detect sanctions evasion

activities through tracking dual–use goods trade via interagency coordination, as well as their analysis and control of the exporter's activity.

427. The MFEA suggested that, to ensure effective identification of assets and funds of designated persons, it conducts preventive and awareness–raising activities for the public and private sectors, exporters, and the research community in relation to the suppression of WMD the export control of dual–use goods.

### *4.4.3. FIs, DNFBPs and VASPs' understanding of and compliance with obligations*

428. Banks and other REs that are members of larger financial groups demonstrated sufficient understanding of UN TFS requirements of PF. Nevertheless, some smaller FIs and DNFBPs displayed limited understanding of the need to verify information against the UN TFS when dealing with the Croatian or EU–Member States' nationals or legal entities. The other REs have a perception that a minimum of 80% of information should match before funds can be frozen and the report filed.

429. Several small FIs (authorised exchange offices, payment institutions, E–money,) and DNFBPs (real estates, lawyers, tax advisors and accountants) stated that in case of a match against UN Sanctions list, they would simply refuse the transaction or exit the customer relationship without filing a report. Some REs confirmed that they will not permit the addition to the accounts frozen under PF–related UNSCRs sanction regime, thus demonstrating a defensive behaviour. These are affected by the less comprehensive understanding of all steps needed to be taken under the freezing mechanism.

430. The mechanism for communicating designations to FIs and DNFBPs is similar to the one for the TF related UN sanction list. The link to the general page of the UNSC and the EU sanctions map are made available on the MFEA website. This approach does not ensure immediate communication of designations and the amendments to the UN sanction lists of designated persons and entities to the REs. This has an impact on the implementation of the relevant UNSCRs by the REs that do not rely on automated sanctions updating and screening mechanisms and had not subscribed to the UNSCRs newsletter on their own initiative.

431. Larger FIs and VASPs use more sophisticated tools and supporting technologies for a timely update of lists of designated persons and entities and their identification. Other FIs and DNFBPs mostly rely on manual checks. The screening frequency of customers within some REs (authorised exchange, payment service providers and lawyers, tax advisors, accountants, casinos, notaries, real estates) depends on the changes of the customer risk profile and the risk level of the customer thus can take place with intervals from once a week to every two years. Hence, these FIs and DNFBPs might not identify a potential match with the UNSCR lists of existing customers in a timely manner.

432. There was some inconsistency in the REs understanding of which the competent authority is to report to when assets are frozen. All three authorities – the AMLO, MFEA, and the MoI were mentioned to be the recipient of the report, sometimes mentioning them all together. As also indicated under IO.10, this is a result of a lack of: (i) established clear mechanism and channels for communication; (ii) reporting form for submitting such reports to the MFEA; and (iii) determined recipient of these disclosures (contact point). It was not evident for the AT whether the MFEA responsible department has clear instructions and knowledge for acting upon the receipt of a report.

433. Outreach activity is conducted within the framework of AML/CFT annual conferences organised by the AMLO with the co–operation of the Croatian Chamber of Economics. Authorities have not provided sufficient guidance to ensure compliance by FIs and DNFBPs with their obligations to implement PF–related UN TFS.

### *4.4.4. Competent authorities ensuring and monitoring compliance*

434. Despite the legislator vesting the supervisory authorities with powers in respect to implementation of measures under the EU, but not the UN framework, the CNB, CFSSA, and Financial Inspectorate demonstrated conducting supervision of implementation of the restrictive measures not only under the EU framework but also the UN.

435. Supervision of implementation of international restrictive measures is carried out through on–site inspections and off–site supervision. The checks on compliance with TFS form part of the AML/CFT on–site inspection. Except for the TA, other supervisory authorities such as the CNB, the Financial Inspectorate and CFSSA, have methodologies for supervision of implementation of the TFS by the REs. On–site inspection includes verification of compliance with the TFS measures on the basis of various criteria, a sample test of customers and transactions, testing of the system to identify the match with the UN Sanction lists. No information is available about the off–site supervisory efforts (statistics, entities, findings, applied sanctions) to evaluate the impact of these on the system.

436. Overall, in 2015–2020 implementation of the TFS measures was included in the scope of 58 on–site inspections (including banks, investment funds management companies, investment firms, life insurance companies, MVTSs, real estate brokers, DPMS, lawyers, notaries, accountants, auditors, tax advisors and TCSP). Based on these inspections, 15 irregularities were identified related to the FIs' internal acts, which were not consistent with the regulations regarding international restrictive measures. It is unclear whether these breaches were identified with respect to TF or PF TFS regimes, but as a result, the assignments to eliminate the violations were issued.

437. AML inspections of Leasing and Factoring companies during the observed period did not include checks on implementation of the UN TFS sanctions. No inspections were conducted over other types of REs, particularly in the gambling sector.

438. In general, as also mentioned in IO.3, at the time of the on–site visit, all supervisory authorities had resource shortages of varied significance for conducting AML/CFT supervision, and the TA did not demonstrate to have dedicated resources in this field. Overall, there is also a need for more frequent supervisory efforts, especially with focus on the weaker performing sectors.

## *Overall conclusions on IO.11*

439. Croatia implements the PF–related UNSCRs through the EU legal framework, which, however, does not ensure timely transposition of the PF related TFS and their implementation without delay (especially on DPRK). While Croatia does not have supplementary national mechanisms to overcome the delay, as concerns mechanisms regarding Iran, there is no practical impact, since the list of individuals and entities is wider in the EU framework and, at a time, already included the respective UN designations. The MFEA did not demonstrate actively performing its role in implementation of the UN TFS.

440. Use of independent mechanisms for ensuring compliance with the UNSCRs by larger FIs (commercial databases) and some other REs (UN newsletters) effectively reduces the impact of the delays in timely implementation of the PF–related TFS by Croatia. The most material sectors of REs demonstrated knowledge and understanding of their PF–related TFS obligations. While no funds were frozen, the REs suggested detecting false–positive matches.

441. Most of the supervisory authorities demonstrated targeting implementation of TSF within the scope of their inspections, but further attention to the topic is required. At the time of the on–site visit, all supervisory authorities had resource shortages of varied significance for conducting AML/CFT supervision, and the TA did not demonstrate to have dedicated resources in this field.

442. The authorities demonstrated supporting PF efforts in a wider manner through the capacity to detect sanctions evasion activities by tracking dual–use goods trade via interagency coordination.

443. The Immediate Outcome is achieved to some extent as despite the delay in transposition of the TFS into the EU framework, in practice, this does not have a material impact in the context of Croatia, and the most material sectors of REs demonstrated knowledge and understanding of their PF–related TFS obligations, implementing these in a timely and efficient manner.

444. **Croatia is rated as having a Moderate level of effectiveness for IO.11.**

# 5. PREVENTIVE MEASURES

## 5.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 4***

a) The level of understanding of ML risks, while in conformity with the NRA findings, varies across sectors, being stronger among banks, MVTS, and to a lesser extent among authorised exchange, VASPs, lawyers and notaries. Other FIs and casinos are aware of the NRA findings, but similarly to the rest of the sectors they could not always explain their risk exposure, in practice. In respect to TF risks, Banks and MVTS's understanding is relatively higher than that of across all other sectors, where understanding is deficient. Overall, all REs could explain their AML/CFT obligations, where FIs could display clear understanding, VASPs – acceptable level, and the DNFBPs – varied, but mostly being at a basic level.

b) Generally, where REs have a limited understanding of ML/TF risks, this has a direct impact on the application of risk–mitigating measures. Banks and MVTS demonstrated advanced practices to application of a risk–based approach, consistent with their risk understanding and assessment of their own businesses' risks. Authorised exchange, lawyers and notaries demonstrated developing own risk indicators, and casinos applying additional risk mitigation measures to online gambling services. The majority of other FIs apply mitigating risks uniformly, without tailoring to their risk characteristics, and confined to pre–determined criteria set out by the supervisory authorities. This conclusion is equally relevant for the other DNFBP sectors, including Real Estate and Accountants.

c) FIs and DNFBPs exhibited different degrees in the application of CDD measures, including the depth and sophistication of ongoing monitoring of business relationships. Relatively stronger performing sectors are banking, MVTS, Authorised Exchange, and online casino providers. VASPs displayed some extent of performance but need time to have measures in place at a satisfactory level. Implementation of CDD requirements to natural persons is adequate, but application of measures to identify BO of a corporate customer raises concerns within all sectors, especially when dealing with complex structures. Most of the REs are conservative and do not use actively electronic identification and verification of a customer. Overall, there is a tendency of relying on banks' CDD as a mitigating measure by various sectors, which puts additional burden on banks and tends to weaken the compliance among the other sectors. Record keeping is performed in line with legislation, where technical gaps so far did not have a material impact.

d) FIs, especially banks, MVTS, E–money and Payment Institutions demonstrated a higher level of effectiveness in applying EDD measures than the DNFBPs. The

application of EDD measures by REs is not always proportionate to the level of observed risks but rather is applied to meet legislative obligation only. (a) With respect to PEPs, there is an over–reliance on personal statements provided by customers with minimal verification of the information and an issue with understanding the difference between requirements for verification of funds and wealth of a PEP. (b) EDD to correspondent banking relationship is applied, but not always with respect to EU–Member States. (c) Risk assessment of new technologies and products is well understood and performed among banks, MVTS, E–Money institutions and Payment Institutions. Others apply in a passive manner and lesser depth because very rarely have changes in provided services. Overall, when introducing the use of new technologies, most supervisory authorities are very involved, which effectively switches the burden of risk assessment from the REs to supervisors. This does not concern the VASPs sector, which is new to the regulatory framework. (d) Banks, MVTS, E–money and Payment Institutions implement wire transfers requirements at a sufficient level. VASPs are not very knowledgeable about the "travel rule" requirements. (e) The most material sector of REs demonstrated awareness about their obligations under UNSCRs, nevertheless, the understanding of the scope of these obligations varies among sectors. (f) All sectors demonstrated thorough understanding of high–risk countries requirements, but when it comes to EU–Member States, application was affected by legislative deficiencies.

e) The STRs align with the risks identified in the NRA to a large extent. The volume of STRs in the banking and MVTS (including the Croatia Post) sectors is largely consistent with the expectations, taking into consideration the materiality and risks present in the sectors than that of the others. STR reporting in non–bank FIs, including authorised exchanges and DNFBPs, casinos, notaries and real estates, is low and may indicate a lack of understanding of reporting requirements or inadequate controls to identify suspicious activity. There are some factors bringing into question the effectiveness of STR reporting, such as: (a) perception of a high evidentiary threshold for filing STR among the REs; (b) instances of submitting STR after a transaction is conducted; (c) instances of non–reporting of attempted transactions. Some sectors are also expected to file a higher number of CTRs, where there are concerns of inappropriate reporting of threshold reports and/or detection of linked transactions. Supervisory authorities focused their attention on the STR and CTR reporting, but the results are yet to be achieved.

f) All REs conduct annual audits to consider the appropriateness of their internal controls and procedures to comply with AML/CFT requirements commensurate to their size, business model and nature of activity.

***Recommended Actions***

***Immediate Outcome 4***

a) Croatia should support REs (FIs, DNFBPs and VASPs) to further deepen their understanding of ML risks and develop the TF risk understanding, including

through also providing the CTF guidance and training to all REs with a focus on sector–specific TF risks.

b) Croatia should ensure that REs improve their firm–specific business risk assessments, based on their own type of activity, client base, etc., and decide on specific and individual risk mitigating measures (including the level of CDD) commensurate to their ML, and specifically TF risks.

c) Croatia should ensure that REs improve their application of CDD, including identification and verification of their customers, and ongoing CDD requirements, based on the dynamic risk profile of a customer. Particular attention should be giver with respect to detection of BO of corporate customers, especially when with complex structures.

d) Croatia should ensure that REs improve their implementation of EDD measures for: (i) PEP identification and verification, including the source of wealth; (ii) conducting an ML/TF risk assessment of the new technology requirements before their application.

e) Croatia should strengthen REs' understanding of CTR reporting and STR requirements through training, guidance and ongoing feedback. This should focus on the quantity of STRs, including clarification on reporting threshold; alignment of STR reporting with AML/CFT risks, especially in low performing sectors; reporting of attempted transactions; reporting STRs before the transaction is conducted.

f) Croatia should take into consideration the specificities of the VASPs sector and provide focused support with regard REs meeting their AML/CFT obligations. Croatia should ensure that VASPs are subject to wire transfer obligations once the "travel rule" solution has been developed. Furthermore, the CFSSA should continue to monitor the potential use of privacy/anonymous products.

445. The relevant IO considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9–23 and elements of R.1, 6, 15 and 29.

## 5.2. Immediate Outcome 4 (Preventive Measures)

446. The assessors ranked obliged sectors on the basis of their relative importance in the context of Croatia, given their respective materiality and level of ML/TF risks (as explained in Chapter 1, 1.4.3).

447. Respectively, **the banking sector and MVTSs are considered the most important** for the materiality and risks present in these two sectors. Both are rated at a level of Medium–high ML/TF risk according to the NRA.

448. The Croatian finance sector is primarily driven by its Banks. The sector's total assets are approx. EUR 62bn., with the 4 biggest banks accounting for around 60% of the market. The majority of banks are members of a banking group. The majority of the total turnover in the provision of money remittance services (96%) is carried out through the non–banking sector. The

total volume of transactions conducted by MVTSs[163] in 2020 respectively amounted to approx. EUR166mln.

449. **Authorised exchange offices, casinos and gambling operators and VASPs are weighted as being important** in Croatia's context. All these sectors are rated at a Medium level of ML/TF risk according to the NRA. The authorised exchange sector and land–based gambling are characterised by high exposure of cash. The online–casino and VASPs sectors are relatively new and developing with a growing interest in the population.

450. The number of licensed authorised exchange offices at the end of 2020 was 1188. The total turnover realised during one year in the sector amounts to approx. EUR 2.5bn. In 2020 the revenue of land–based casinos was estimated at the level of EUR 18 mln., and the revenue of online casinos – EUR 106 mln. The volume of VASPs transactions was estimated at a level of EUR 62 mln. in 2020.

451. Among the other sectors, as presented in Chapter 1, **housing savings banks, leasing companies, electronic money institutions, lawyers, accountants, tax advisors, notaries public, real estate brokers and dealers in precious metals and stones are weighted as being moderately important** in Croatia's context based on their materiality and risks. The rest of the FIs and DNFBPs are considered to be of **low importance.**

452. The conclusions under IO.4 are based on written documentation (including processes and procedures, statistics, case examples) provided by all four supervisory authorities, meetings with supervisors and relevant authorities, and interviews with a range of private sector representatives from the financial, VASPs and non–financial sectors. Private sector representatives met included a sample of the largest firms and professions in a combination of higher ML/TF risks as was presented by the supervisory authorities. These in total represent a significant share of the market in terms of assets.

453. To note that most of the technical deficiencies identified do not have a strong impact on the compliance of some of the sector's ability to adequately apply AML/CFT preventive measures commensurate with their risks and report suspicious transactions. These are subject to follow–up analysis, and therefore, no recommended action is set under the effectiveness section.

### *5.2.1. Understanding of ML/TF risks and AML/CFT obligations*

*Financial Institutions*

454. The level of understanding of ML risks, while conforming with the NRA findings, varies across sectors depending on the type of activity and geographical footprint. FIs part of an international group structure are more sophisticated in articulating their specific and individual ML risks. Other FIs rely primarily on information published or distributed by competent authorities. In respect to TF risks, Banks and MVTS's understanding is relatively higher than that across all other sectors, where understanding is deficient. The understanding and awareness of TF risks and vulnerabilities were not demonstrated across these other sectors. Particularly in respect of FIs that provide services in Croatia, the understanding is that there was zero or minimal TF risk exposure.

455. Banks are aware and understand the 2020 NRA and generally agree with the risks identified in the NRA. Banks are able to articulate their views on their exposure to ML risks and

[163] This includes also figures for the Croatia Post.

vulnerabilities. They confirm observing risks related to the cash exposure, tax evasion, fraud (including cyber–fraud), corruption, non–residents and fictitious companies featuring in the NRA and the known typologies. Larger Banks that are part of an international Group have a broader understanding of ML/TF risks and the practical application of the NRA, as they will encompass a wider risk exposure due to the Groups' global coverage.

456. The Banks' understanding in respect to TF risks is more sophisticated than other sectors, though it is still considered lesser than the understanding of ML risks. Banks focus on TF risks identified within the NRA and are unable to articulate other types of TF risks to which they are or could be exposed either as a sector or a separate Bank.

457. Banks can discuss conducted internal business risk assessments, which supplement the findings of the NRA. They carry out their own risk assessments, and these include factors such as customer risk, product/service risk, and geographical risk. The risk assessments are comprehensive and take into consideration the NRA and also the Bank's own internal data. Most of the banks demonstrated that their assessments are updated regularly, given that they are required by law to undertake an annual review of all their procedures and policies. Where the Bank is part of a larger Group, risk assessments generally also take into account the groups' assessment of risks.

458. Banks demonstrate a clear understanding of their AML/CFT obligations and can articulate these. Banks assess risks of all customers prior to establishing the business relationship. Most banks noted they had a conservative risk appetite, given their client base is primarily comprised of Croatian nationals. Some banks also have restrictions on the type of activity they will accept from their corporate clients to limit their risk exposure, e.g., they would not bank crypto related activities.

459. The MVTS sector clearly understands their ML/TF risk exposure, given the nature of their activity. This sector is the most knowledgeable in articulating very specific trends and typologies to which they are exposed. In addition to tax evasion, as identified within the NRA, the MVTS sector also highlighted other risks that they consider as high, such as drug and human trafficking. The MVTS sector evidenced transactional and client activity assessments conducted on a monthly and quarterly basis, which had resulted in various typologies reported to AMLO and other relevant authorities. For example, some MVTS' have identified migrant smuggling risks linked to transactions to and from certain neighbouring countries. Therefore, they have highlighted these countries as posing a higher risk within their own internal methodology and within their systems. Another example is the identified VAT fraud typology linked to a neighbouring country. Specifically, on TF, the MVTS sector is the most knowledgeable and has demonstrated the most sophisticated controls to identify and monitor TF risks. The sector confirmed that they had increased their controls and transaction monitoring indicators in 2018, arising from identified trends. The sector was also able to articulate typologies and trends with potential TF exposure, e.g., the identification of a higher volume of transactions, sometimes in multiple smaller amounts, to certain countries with a perceived higher risk of TF or conflict zone.

460. The MVTS sector was able to explain their AML/CFT obligations, with all having most of these requirements integrated into the systems and databases used by the EU Payment Institution with which they have agency relationships. The MVTSs based in Croatia are primarily agents of two EU Payment Institutions and are subject to their group policies and procedures.

461. Although less sophisticated, the authorised exchange sector demonstrates an understanding and awareness of ML risks relevant to its activities. Given the nature of its

activities, the sector is knowledgeable particularly of the risks posed by the use of cash, including related to small scale (street) drug trafficking. The sector has also identified that one of its main vulnerabilities is the potential abuse by criminals who could evade CDD by using multiple exchange offices and transacting smaller amounts. With respect to their AML/CFT obligations, the exchange office sector demonstrated it could articulate the legal requirements to which it needs to adhere, including changes to these, e.g., the reduction in the threshold when CDD applies to cash transactions.

462. The house savings banks, leasing, factoring and E–Money sectors' knowledge of ML risks is more limited. The leasing and factoring sectors specifically consider that there is no ML or TF vulnerability or risk exposure to their activity or their own organisation. However, the sectors were unable to articulate the reasons for these views, or how they considered the NRA in their organisations. Similarly, the House Savings Banks noted that given their focus was primarily on the domestic market, aimed at Croatian nationals, their ML exposure was minimal. These sectors demonstrate a basic level of understanding of their AML/CFT obligations, with most REs following the generic and basic prescribed requirements in law.

463. The E–Money sector's understanding was varied, primarily due to the wide range of activities offered by the sector. REs that focus on telecom services in Croatia have less of an understanding and awareness of potential ML risks, as opposed to firms that provide a wider range of e–money services globally. The level of understanding of the AML/CFT obligations varied significantly within the sector. Smaller E–Money institutions, whose target was the Croatian market, demonstrate a very basic understanding of the obligations. Similarly to other sectors, these REs will solely follow the basic prescribed requirements in law without consideration of their own risks. On the contrary, E–Money Institutions that are part of a larger group, or operate internationally, have a more sophisticated and comprehensive understanding of their AML/CFT obligations. This also includes a better understanding of the measure available to comply with their obligations, e.g., the use of electronic identification for non–face to face customers.

464. All other FIs confirmed awareness of the 2020 NRA and its contents. They also agree with the assessment carried out by the NRA. However, only a small number of these other FIs were able to explain how they had made use of the NRA as part of their own policies and procedures. The majority of these FIs demonstrate a clear understanding of their AML/CFT obligations, in particular the Payment institutions.

*DNFBPs*

465. As explained further, the level of understanding of ML risks across DNFBP sectors varies. While being aware of the NRA findings, the DNFBPs are not always able to explain their own risk exposure in practical terms. The DNFBPs sectors' knowledge and awareness of TF risks are limited to the contents of the NRA (which does not assess the ML/TF risks pertinent to these sectors and do not distinguish between the ML and TF vulnerabilities in these sectors). There is no understanding of potential TF risks or vulnerabilities to which their businesses could be exposed. Similarly, DNFBPs understanding of their AML/CFT obligations varied across sectors and within sectors.

466. The Casinos are aware of the NRA and can articulate its contents. However, the practical application and understanding of ML/TF risks are unsatisfactory. The sector is unable to explain the ML/TF risks it is exposed to, given the nature of its activities, how it makes use of the NRA, and it does not demonstrate that periodic risk assessments or trend analyses are conducted.

467. With respect to the AML/CFT obligations the sector is versed in the legal requirements. But similarly, the implementation of these, in practice, is not clear. The Casinos implement very basic controls to ensure a minimum of legal compliance, and there is no consideration of a risk–based approach based on specific ML/TF risks identified by the NRA or by themselves individually.

468. The lawyers and notaries do exhibit some understanding of ML risks and are aware of the 2020 NRA, although some indicated that the two sectors are very different and should not have been grouped together when conducting the NRA. These sectors primarily highlighted tax evasion as their main risk. Both sectors demonstrated adequate understanding of their AML/CFT obligations, and evidenced their onboarding procedures, requesting documentation from clients to verify the customer and BOs.

469. The real estate brokers recognise the ML exposure of the real estate sector in Croatia. They consider that the market exposure itself does not have considerable bearing on the level of potential ML abuse of the real estate brokerage sector itself due to the following three factors: (i) no compulsory obligation for operating through the real estate brokers to purchase immovable property, and only 1/3 of operations are conducted through them; (ii) considering the AML/CFT compliance mechanisms put in place for the real estate brokers, the criminals would rather avoid addressing the regulated sector; and (iii) the real estate brokers are not themselves involved into the financial transactions, rather their role is limited to a simple introduction of the seller and acquirer. These factors are giving the comfort of protection from ML abuse to the real estate brokers' sector. They could not articulate how in practice their services could be exploited for ML purposes and indicated their own ML/TF risks to be low. The AT views diverges from the sector's, primarily because the NRA and other typology work has clearly evidenced that the purchase and sale of real estate is a high–risk product that has been associated with corruption, hence, the sector will have an inherent exposure to ML/TF risk. This demonstrates that the sector does not have an understanding of its risks exposure. Similarly, the understanding of their AML/CFT obligations, while it varies across the sector, on average, is at a basic level.

470. Accountants, Tax Advisors, and partially the DPMSs and TCSP, similarly to other DNFBP sectors, do not demonstrate sufficient understanding and awareness of ML risks specific to the nature and size of their businesses. Nevertheless, the Accountants and Tax Advisors confirmed a basic understanding of their AML/CFT obligations and compliance with the legislative requirements: to conduct a self – assessment of their business ML/TF risks and update their internal risk assessments, policies and procedures, including on the basis of the two iterations of the NRAs.

*VASPs*

471. The VASP sector shows an acceptable level of understanding of risks and understanding of their AML/CFT obligations. VASPs highlighted some of the risks they consider they are exposed to, such as potential fraud or scams, tax evasion, and the purchase and sale of drugs. During the on–site, one VASP specifically referred to using and offering privacy/anonymous coins, though the legislator had prohibited anonymous products and services[164]. The VASP was unable to adequately demonstrate the risk exposure of such products or how these products would permit compliance with AML/CFT obligations.

472. This sector is considered relatively new to the scope of AML/CFT, and it is still working with CFSSA – its supervisory authority, to ensure a thorough understanding and adequate

[164] AMLTFL, Art.54

application of its compliance arrangements. Not all VASPs operating in Croatia have yet identified themselves filing a notification to the CFSSA, and hence it is unclear to which extent these have developed their ML/TF risk understanding, took into consideration the risks detected at a national level, and also understood and aligned their working practices to their AML/CFT obligations.

### *5.2.2. Application of risk–mitigating measures*

473. All REs are required to implement AML/CFT preventative measures commensurate to their ML/TF risks. There is a legislative requirement to conduct ML/TF risk assessment; establish policies, controls, and procedures commensurate to their ML/TF risks; regularly update a list of indicators of ML/TF risk exposure, etc. However, the extent to which these preventative measures are satisfactorily applied varies between and within sectors. Larger FIs demonstrate advanced practices to application of a risk–based approach, consistent with their risk understanding and assessment of their own businesses' risks. The majority of other FIs apply mitigating risks uniformly, without tailoring to their risk characteristics. They apply the mitigating measures explicitly noted within the legislation, guidance notes, red flags, typologies and other indicators issued by their supervisory authorities. This conclusion is equally relevant for most of the DNFBP sector.

474. With respect to TF, as noted above, the understanding of the risks is very limited for most sectors, excluding Banks and MVTS, and therefore the majority of REs rely solely on TFS sanctions screening as their only TF risk–mitigating measure. The assessment team considers this sole measure to be not enough to mitigate TF risks.

475. Non–bank FIs (e.g., authorised exchange, investment firms) and DNFBPs (e.g., legal professions, real estate brokers, casinos, DPMS) rely to some extent on the Bank's risk–mitigating measures in respect to conducting CDD and monitoring transactions, as assurance for their own risks. The instances observed are such as customers are: (a) re–directed to banks for conducting a transaction, or (b) the bank is in the chain of multi–stakeholder services. These are the following transactions: exchange of currency in large sums and by non–residents (where customers are re–directed to a bank); charging the wallets of on–line casinos via banks transaction (where a bank is a gatekeeper); acquisition of precious stones and metals above the set threshold using a bank transfer (idem), non–cash real estate purchase (idem); or checks and verifications at the stage of legal person formation (idem) (see IO.5). Whilst in certain cases, this can be considered good practice and good mitigating measures, given that it adds another level of control; the level of displayed reliance on banks is of concern as it places an undue burden on the banking sector, and it weakens the overall effectiveness of the compliance within sectors.

*Financial Institutions*

476. FIs supervised by the CNB and Financial Inspectorate did articulate a better understanding of risk–mitigating measures than others. The specific risk–mitigating measures introduced by the Croatian authorities as a result of the 2016 NRA (see IO.1) and by the key indicators published by supervisory authorities are, in general, well understood and implemented. This appears to be the result of the extensive engagement carried out by the supervisory authorities with its sectors to raise awareness in these areas (see IO.3).

477. Banks and MVTS with international business or part of international group structures have implemented more comprehensive internal systems and controls to mitigate ML/TF risks than others that are not.

478. An example demonstrated was that Banks implemented enhanced measures when dealing with customers non–face to face, such as requiring new customers to deposit money through a transfer from another credit institution subject to equivalent AML/CFT controls and not accepting cash as the first transaction. Other measures implemented by banks are diligence applied to mitigate risks related to detected I–typology. Currently, business relationships with legal persons are scrutinised, and additional due diligence measures are applied. This also had an effect on the increase of STR reporting by the sector. Supervisory findings suggest a positive dynamic in strengthening its business and individual customer risk assessments and systems commensurate to the size and the type, scope and complexity of banks' operations.

479. The MVTS evidences a sound knowledge of sector specific risks and noted trend analysis carried out within their firms. These trend analyses resulted in additional key indicators, further to those already provided by the Financial Inspectorate. This sector evidenced periodic analysis of its data that derived from the implementation of new policies or changes to existing policies, e.g., the sector regularly assesses the country risk within their methodologies and will assign a higher risk to any country they have identified that could be potentially abused by criminals for matters such as drug or human trafficking. This sector has evidenced specific internal training on risks identified, for example training on ISIS and Foreign Fighter Risk.

480. The authorised exchange sector describes its risk–mitigating measures which are mainly based on the risk indicators and typologies provided by the supervisory authorities and which inform application of a risk–based approach. Some authorised exchange offices mentioned developing their own indicators, e.g., operations in small dimensions of currency, which they suggested to be linked with a street drug market. Some mentioned applying additional, centralised transaction monitoring measures to analyse the clients and their behaviours and find linked operations conducted through their outlet net (e.g., detecting customers using different outlets, a small amount of money to structure transactions etc.). Authorised exchange offices described taking steps for strengthening the transaction monitoring through introducing the indicators into the IT system supporting their operations.

481. Smaller FIs still demonstrated they had some risk–mitigating measures, though these, in general, are less structured and sophisticated and not always risk–based. This is especially observed among the FIs with relatively weaker ML/TF risk understanding, as described above.

*DNFBPs*

482. DNFBPs demonstrated a basic level of application of mitigating measures commensurate to their risks but with varying degrees among sectors. Generally, DNFBPs risk–mitigating measures are confined to be pre–determined by key indicators provided by supervisory authorities, with minimum effort to establish specific ones on the basis of individual business risk assessment.

483. The Casinos follow the basic risk mitigation measures as prescribed in the law. When dealing with on–line gambling – a relatively new and developing sub–sector, to mitigate the potential risks, additional requirements apply: (i) when onboarding a customer identification and verification is to be conducted upon physical presence in the outlet of the casino, where also a video identification is conducted; and (ii) the player's wallet should be toped up only via a bank transaction. As concerns the land–casinos, these are perceived by the sector as a higher risk product than the on–line casino. The main risk mitigation measures are focused on monitoring transaction thresholds and detection of a basic scheme of returning casino chips with no game performed (this is done using audio/video person recognition tools). The latter is a scenario where the casino will reject the transaction.

484. The lawyers informed to not only apply the set indicators and red flags as provided by the regulators, but also have made further efforts and developed additional risk indicators (e.g., fictitious invoices) which take into account the NRA findings on the top three threats. The indicators are now implemented into their internal enactments.

485. Similarly, the notaries have presented some trends they themselves observed and confirmed applying EDD in such instances. These are the observation of ML schemes: (i) pretending an inheritance to legitimise their financial resources; (ii) unsubstantiated transfers of ownership within a company; and (iii) acquiring a company that was inactive for some years.

486. Concerning the accountants and tax advisors, real estates, DMPSs and other DNFBPs, it is observed that they act within the scope of legislative requirements to conduct risk assessments, to apply commensurate risk–based measures, but could not articulate on and demonstrate the effect of these in the practical terms. They articulate very basic procedures when onboarding customers.

*VASPs*

487. VASPs are a newly regulated sector and are still developing their risk–mitigating measures. The CFSSA is working with the sector to provide feedback on their internal controls, compliance arrangements, etc. To note again that this sector was unable to describe any risk–mitigating measures in respect to privacy coins, though the legislator had prohibited such a product.

### *5.2.3. Application of CDD and record–keeping requirements*

*Application of CDD*

488. REs could all recite the CDD legal requirements, including when dealing with new customers or monitoring established business relationships. The extent of how these requirements are put, in practice, differs between and within the sectors. The Banking and the MVTS sectors displayed a better understanding and more comprehensive policies and procedures for implementation of CDD measures. Nevertheless, the summary of the supervisory findings suggests fulfilment of CDD requirements is an issue in the MVTS, authorised exchanges, accountants, auditors, and DPMS sectors.

489. The AT observed a potential link between the understanding of CDD obligations and quality of their implementation and the carried–out supervision. It was noted by some FIs and DNFBPs, that in the last 2 years, there had been an increased awareness and focus on compliance with CDD requirements. This was also confirmed by the supervisory efforts made by the CNB and the Financial Inspectorate. They have conducted a number of on–site and off–site inspections to supervised entities and detected weaknesses in the adequate application of preventative measures, including CDD requirements. A number of sanctions were applied, and follow–up checks were conducted that confirmed improvement in application of these obligations.

490. Generally, all the REs could describe the taken steps, collected documents, and conducted checks when dealing with a new customer. Most FIs and all DNFBPs suggested to apply face to face CDD to all new customers. In March 2021, the supervisory authorities issued guidance to allow the use of electronic verification, however, most sectors advised that they had not implemented such an approach into their internal policies and procedures and would continue to request face to face verification. Only some of the Banks, VASPs, and Payment Institutions suggested having already implemented electronic identity verification systems.

491. All REs demonstrated an adequate understanding of the CDD requirements that apply to customers who are natural persons. Some of the REs suggested being also vigilant towards the detection of a BO of a natural person. In particular, banks, MVTS and authorised exchanges indicated to occasionally observe situations when the customer is accompanied by another person. In these instances, additional checks are made to understand the role of a third person.

492. As concerns corporate clients, the majority of REs advised that CDD is carried out on the direct customer (the corporate) and the ultimate beneficial owner(s) only. Where the corporate client is comprised of multiple layers of shareholders, CDD is not always conducted on the indirect BOs. This issue was identified similarly for FIs and DNFBPs, including Banks, though the degree of understanding of this matter was mixed across and within sectors. E.g., one of the Banks noted that this had been one of the deficiencies identified by its supervisory authority, and which resulted in a sanction against the Bank.

493. Regarding ongoing CDD, all REs regularly conduct monitoring of customers, but with varying levels of sophistication which was mostly due to the profile of their services and a client base. The largest banks apply complex measures and benefit from sophisticated IT systems. Customers are also periodically re–evaluated, with a frequency that depends on the level of the risk given to the customer. High–risk customers are re–evaluated on an annual basis, and if medium – biennially. The reviews imply requesting full CDD data from a customer, its analysis and verification with the historical knowledge about the customer, including checks whether the information and documentation already held is up–to–date and accurate. This also includes automated checks of matches with the PEP and TFS lists and any changes in the geographical risks. The MVTSs monitor the customer base paying attention to the customer's typical behaviour, e.g., in terms of frequency, amount and addressee (person and geography) of transactions. Checks are conducted to collect additional information about the customers transacting repetitively, including on the basis of open–source information (an example of detection of a suspicious transaction was provided on–site). The authorised exchanges apply measures similar to the MVTS.

494. With respect to the casinos, the monitoring mechanisms applied to land–based and on–line casinos vary, the latter being stronger. They apply a customer risk assessment dynamic scoring system that is sensitive to any change in the customer's behaviour and actively utilises IT systems, with a wide range of key factors put into the algorithm, for monitoring of customers. The other DNFBPs explained rarely establishing a business relationship with the customers due to the nature of the provided services hence rarely applying customer monitoring measures, in practice.

495. VASPs indicated that due to the nature of the provided services, all customers are scored as medium and high risk only. The customer monitoring is conducted with use of IT systems, which are evolving gradually in parallel with the knowledge and experience gained by the sector. Nevertheless, taking into consideration that the sector is new to AML/CFT requirements, time is required to develop the measures in place to a satisfactory level.

496. All REs are aware of the legal obligation to ensure that CDD is completed before a customer is onboarded, and all REs confirmed not to onboard the customers without full CDD. REs also noted that if a client challenges the need to provide CDD, it raises a red flag and could be considered suspicious. However, very few noted that this would trigger an investigation and potential filing of an STR, but instead, REs will just reject the client. Discussing the existing customers, FIs mentioned that if full information about the transaction is not provided, it will not be executed – funds will not exit the account. If on the account, the funds respectively will not be

made available to the customer before all information is collected and verified. The DNFBPs confirmed that in these circumstances the transaction/agreement arrangements would not be accomplished/validated.

497. Concerning the application of simplified CDD measures, with the exception of the E–Money sector that has specific legal provisions that allow SDD, these are applied by REs in very limited instances and are based on the level of the risk assigned to a customer. Most of the REs mentioned that they never apply simplified measures to non–residents, often explaining this by the widely known I–typology. Some sectors, such as VASPs, noted not applying simplified CDD at all due to the inherent risk profile of their customers. There was a misunderstanding among the lawyers, some of them mentioning that they do not apply simplified CDD measures because their own sector was assessed in the NRA as at a level of Medium ML/TF risk. This seems to be a misinterpretation of the legislation, which requires taking into consideration the NRA outcomes in terms of assessment of the customer's risks when considering application of SDD and not the sector's own risks.

*Record keeping*

498. All REs can recite the legislative record–keeping requirements, which is to hold CDD and transaction data for at least 10 years. However, the requirement to keep records on results of any analysis undertaken is limited to analyses done in relation to complex and unusual transactions and does not cover records on other types of analysis. The completeness of CDD information subject to retaining is also affected by the misunderstanding on the application of CDD to direct and indirect BO. There have been no breaches identified by the supervisory authorities in respect to this requirement. No complaint was also expressed by the LEAs in terms of availability of all necessary information to support the investigation with necessary evidence.

### *5.2.4. Application of EDD measures*

499. All REs could describe legal requirements with respect to application of EDD measures below described elements, as pertinent to their sectors and the type of provided services. Some REs, mostly FIs, demonstrated a higher level of effectiveness in applying EDD measures than the DNFBPs. It was observed that the application of EDD measures by REs is not always proportionate to the level of observed risks but rather was applied to meet the legislative obligation only.

*PEPs*

500. Overall, FIs and DNFBPs have an adequate understanding of the definition of PEPs, including family members and close associates. The issues noted above in respect to CDD on the BO has a bearing on effectiveness in identifying PEPs. Banks and MVTS specifically did demonstrate a better understanding of the requirements.

501. While the legislative ambiguities are detected as described in the TC Annex, all FIs and DNFBPs considered that both domestic and foreign PEPs are covered, and they apply respective measured to both. There is nevertheless no understanding displayed that the additional measures to CDD should apply to domestic PEPs, where a higher risk business relationship is detected. The REs apply these in all circumstances, which is, in effect, a stricter approach than that expected by the FATF Standards. Some FIs are conservative and suggest doing business only with domestic PEPs.

502. Nevertheless, the majority of FIs and DNFBPs did not demonstrate a good understanding and/or implementation of requirements concerning the verification of the source of wealth and

source of funds. The majority of the FIs and DNFBPs are aware of the requirement to establish the source of funds, but there were many cases in which some FIs, and especially the DNFBPs, did not demonstrate awareness of the separate requirement to establish and verify the source of wealth. Generally, there is a misunderstanding with the definition of source of funds vs source of wealth.

503. Disclosure of information on the PEP status of a customer is part of a standard identification of a customer, e.g., part of "know your customer" fact questionnaires. Some FIs and all DNFBPs displayed overreliance on the self–declaration of a customer to disclose its status, with no further independent checks conducted to detect instances of non–reporting and to apply respective additional measures. Most of them conduct independent verification only when having a suspicion. This undermines the effectiveness of detection of PEPs and application of respective measures.

504. Some FIs and DNFBPs advised of information publicly available in respect to domestic PEPs, e.g., reference to a PEP register detailing the wealth of the PEP, and ones that are familiar with the public information rely solely on this data, without any verification. As concerns foreign PEPs, the issue of reliance on a self–declaration is more present. This will be typically verified by FIs such as Banks, VASPs, MVTS, Payment Institutions and E–Money that have adequate resources to utilise third–party screening tools. In addition, where the FIs are part of a larger group, they also utilise Group resources for the verification of PEPs and the source for funds and wealth. Authorised exchanges, real estates, and casinos suggested conducting manual opensource (internet) information checks on PEPs. This method is not adequate, especially when it concerns the real estate agencies dealing with foreign PEPs – indirect acquirers of a property.

*Correspondent Banking*

505. The Banking sector does offer correspondent banking services, including *nostro* and *vostro* accounts. The sector does not offer payable through accounts, though it does make use of this arrangement with other banks for its clients.

506. Banks that offer these services demonstrated a good understanding of the enhanced ML/TF risks and AML/CFT requirements. The EDD entails obtaining further information on the customer, including the nature of the activity and reason for the transaction and verification of the source of funds. Some banks that are part of a group informed that the decision on engaging and termination of the correspondent relationship is a decision taken at a group level and not by the banks themselves. The AT specifically scrutinised the effect of the legislative limitations with respect to application of additional measures to correspondent relations set with EU Member States. While some follow the set regulatory framework, others informed of conducting an annual risk assessment of their parent banks and other respondents from EU countries exchanging questionnaires. These business relationships are established by the senior management's approval and are subject to enhanced monitoring, including a greater frequency and more intense scope of reviews.

507. There was no indication of similar correspondent–type relationships outside of Banks.

*New technologies*

508. Most REs acknowledged the legal requirement to carry out an ML/TF risk assessment for all new products, services, delivery channels and technologies before implementation. FIs with international business or part of international group structures (e.g., Banks, MVTS, E–Money Institutions and Payment Institutions) exhibited a more sophisticated approach to the

assessment of new technologies. Some of the non–bank FIs and especially the DNFBPs generally advised that these assessments are uncommon, in practice, as they very rarely launch new products or services. This was one of the reasons why only very few of them could actually formulate the details of these assessments or provide specific examples. The risk assessment of existing products is conducted within the scope of a standard annual assessment of the ML/TF risks[165], which is submitted to the respective supervisory authority. With respect to the VASPs, whilst this sector commonly utilises blockchain or other distributed ledger technology, the sector is not familiar with the requirement to carry out ML/TF specific risk assessments on new technologies.

509. Supervisory authorities take over an important role in supporting the REs to ensure that, e.g., the ML/TF risks when using new technology/delivery channels in the country are minimised. This is achieved through setting a quite prescriptive regulatory framework for some business practices. Any new business practices need to be discussed and agreed upon with the relevant supervisory authority before being launched. As a consequence, it is observed that such practices would create reliance of the private sector on the supervisory authorities, and in effect, switch the burden of risk assessment onto the latter.

510. An example of such a prescriptive regulation, which also has its important benefits of supervisory support, is in respect to authorised exchange offices. The services can be provided only using an IT system that is subject to prescribed specifications in law. The CNB review and approve the system prior to the authorised exchange office permitted to make use of it. Hence, it appears that the risk assessment of this technology is conducted by the supervisory authority rather than by the RE.

511. One of the examples, as also discussed above, was the introduction of electronic verification for non–face–to–face customers. The requirements to implement such measures have been prescribed by the supervisory authorities through the issuance of harmonised guidance on behalf of all supervisory authorities, and that is applicable to all sectors. Hence, sectors are not required to carry out their own individual ML/TF risk assessment. This new measure has been taken conservatively by the private sector but implemented by some banks and sectors, which provide primarily online services, such as VASPs. These REs have more sophisticated tools, e.g., online verification of identification, that allows a smoother implementation.

512. There are some examples of new technologies implemented by the private sector, which is conducted independently (e.g., banks and a casino). A large bank that is also a part of a larger group is launching a new investment product that underwent 2 years of testing and included an assessment against ML/TF risks. This product was tested not only at the Croatian bank's level but also underwent a group assessment. Another example was another large bank launching the sale of products via mobile phone. This service was launched after a thorough assessment of potential ML/TF risks and was offered to the public after necessary adjustments were made on the basis of the risk assessment findings. A casino involved in on–line gambling advised that when they launch a new game before the product is offered to the customers, this undergoes various stages of certification in Croatia and internationally, where the data protection and AML/CFT measures are also assessed. With respect to the casino the doubts remained as the element of the ML/TF risk assessment was not entirely evident.

[165] AMLTFL, Art.12 required assessment of risks of customers, countries or geographic areas, products, services or transactions, and delivery channels.

*Wire transfers*

513. Banks, MVTS, Payment institutions and E–Money institutions exhibited sufficient knowledge of the wire transfer requirements. Based on Croatia's compliance with the EU Wire Transfer Regulations (2015/847), these sectors are aware of the need to obtain and transmit data with respect to the originator and beneficiary of transactions. Croatia does not apply the *de minimis* threshold.

514. MVTSs' are all agents of global providers and therefore make use of their systems and software for screening of transactions. These software solutions allow firms to execute or block a transaction when necessary due to, e.g., incomplete information. Banks also indicated the use of systems that have integrated controls to ensure compliance with the EU wire transfer regulations.

515. As part of its supervision, the CNB uses a third–party tool for transaction analysis. This tool analyses the transaction data, including compliance with the wire transfer requirements. No significant deficiencies have been identified by the supervisory authorities.

516. Regarding VASPs, they are monitoring the market for new solutions in providing the services but are not very knowledgeable of the need to find a technical solution to address the "travel rule" issue. This mostly is because of the very new, developing nature of their involvement to the AML/CFT matters and because the "travel rule" has not yet been integrated into the legal framework.

*Targeted financial sanctions*

517. The most material sector of REs demonstrated awareness about their obligations under UNSCRs, nevertheless, the understanding of the scope of these obligations varies among sectors.

518. Larger banks and MVTS demonstrated sufficient understanding of TFS requirements and make use of commercial databases to screen customers periodically. Other sectors are generally aware of the obligations in relation to TFS, though some REs from these sectors rely primarily on manual checks at the point of onboarding a customer. REs that rely on manual screening very rarely screen the customer on a periodic basis and do not have adequate controls in place to screen their databases when the sanctions lists are updated.

519. In addition, the information articulated by RE's ranged from confusion between country related sanctions to designated individual sanctions and lack of clarity on which sanctions lists were applicable. References were made to EU, UN lists and also to OFAC and FATF restrictive measures.

520. The issues noted above in respect to RE's understanding of BOs also affects the implementation of TFS, as not all BOs are subject to TFS screening. (See also IO.10 and IO.11)

*Higher risk countries*

521. All FIs and DNFBPs demonstrate a thorough understanding of higher–risk countries and measures to be applied when dealing with such. They are aware of the FATF publications on high risk and other monitored jurisdictions, and the majority are also aware of the EU Regulation (2020/855) on higher–risk countries.

522. FIs involved in international business or part of international group structures (e.g., Banks, MVTS, E–Money Institutions and Payment Institutions) exhibited more sophisticated measures in this area. These REs supplement the official information from the FATF and the EU with other information such as the Transparency International's CPI, the Financial Secrecy Index, BASEL

AML index, etc. Furthermore, these REs usually have automated systems to identify transactions to or from higher risk countries. Other FIs and DNFBPs rely on manual checks.

523. However, some REs consider EEA countries as posing a low risk by default, which is not based on actual risk. Even though EEA countries are meant to hold equivalent legal standards based on the EU anti–money laundering Directive, the application of such standards, and the potential risks depending on the type of activity, volume, etc., in addition to any trends identified; should still be assessed by firms as part of their own specific and individual business risk assessments. This is a reflection of a deficiency as described under R.19.

### *5.2.5. Reporting obligations and tipping off*

524. The volume of STRs in Banking and MVTS (including the Croatia Post) is considered to be more consistent with the expectation, taking into consideration the materiality and risks present in the sectors than that of the others. STR reporting in some sectors is considered to be low and may indicate a lack of understanding of reporting requirements or inadequate controls to identify suspicious activity. Supervisory authorities focused their attention on the STR reporting among the REs, but the results are yet to be achieved.

525. The STRs align with the risks identified within the NRA to a large extent. These are relevant to detection of tax evasion and corruption, risks related to non–residents and use of fictitious legal persons, migrant trafficking, but when it comes to trafficking of drugs, banks suggested it is hard to detect such schemes, the others, such as MVTS and Authorised Exchange offices suggested observing operations that are related to "street sales".

526. In general, across all sectors, there is a perceived sense of a high threshold before being able to file an STR. A significant number of REs, particularly smaller ones, have advised that they understand that they are required to investigate and have a tested case before submitting an STR. Specifically for TFS related STRs, it is the REs' understanding that a minimum of 80% of information should match before an STR can be filed.

527. The REs are required to file the STR promptly, which is implemented especially by the major producers of the STRs. There is, however, a legislative provision suggesting that where REs cannot report prior to the carrying out of a suspicious transaction (due to the nature of the transaction or for other justifiable reasons –which are not defined), the reporting shall take place after the transaction is made. On the basis of the interviews and some case examples, the AT observed this provision to be applied occasionally, especially in circumstances when transfer of funds or exchange operations are concerned. This was explained as a measure to avoid tipping off the customer, but the AT has doubts about the manner of application of this legislative provision. This reporting behaviour also affects the successful detection of cases, as further described in IO.6.

528. In addition, Non–Banks and DNFBPs do not generally have a clear understanding of the duty to file STRs in respect to attempted business relationships and transactions. This can be evidenced by the number of STRs relating to attempted transactions – an average of less than 0.5% during the last 5 years. The Bank sector's average during the last year is 13%.

**Table 5.1: Number of STRs per sector for ML, TF and attempted transactions[166].**

| | 2015 | | | 2016 | | | 2017 | | | 2018 | | | 2019 | | | 2020 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ML | FT | AT[167] | ML | FT | AT | ML | FT | AT | ML | FT | AT | ML | FT | AT | ML | FT | AT |
| Financial Institutions | | | | | | | | | | | | | | | | | | |
| Banks | 663 | 7 | 97 | 771 | 5 | 153 | 612 | 4 | 63 | 630 | 4 | 90 | 693 | 11 | 120 | 2243 | 11 | 109 |
| MVTS[168] | 0 | 0 | 0 | 46 | 0 | 0 | 37 | 0 | 0 | 49 | 0 | 9 | 132 | 0 | 0 | 117 | 0 | 0 |
| Croatian post[169] | 66 | 0 | 0 | 96 | 0 | 0 | 118 | 0 | 0 | 4 | 0 | 0 | 41 | 0 | 0 | 55 | 0 | 0 |
| E–money | 1 | 0 | 1 | 0 | 0 | 0 | 52 | 0 | 49 | 11 | 0 | 0 | 12 | 0 | 0 | 9 | 0 | 0 |
| Exchange | 6 | 0 | 0 | 1 | 0 | 0 | 2 | 0 | 1 | 17[170] | 0 | 0 | 2 | 0 | 0 | 4 | 0 | 0 |
| Housing savings banks | 5 | 0 | 0 | 14 | 0 | 4 | 0 | 0 | 7 | 6 | 0 | 4 | 6 | 0 | 2 | 8 | 0 | 0 |
| Insurance sector | 0 | 0 | 0 | 4 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 |
| Securities sector | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Investment firms | 4 | 0 | 1 | 6 | 0 | 2 | 6 | 0 | 0 | 0 | 0 | 0 | 9 | 0 | 3 | 3 | 0 | 0 |
| Credit cards issuers | 1 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Leasing | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 |
| Total | 749 | 7 | 101 | 944 | 5 | 163 | 830 | 4 | 120 | 724 | 4 | 104 | 897 | 11 | 125 | 2445 | 11 | 109 |
| DNFBPs | | | | | | | | | | | | | | | | | | |
| Notaries | 11 | 0 | 2 | 5 | 0 | 1 | 4 | 0 | 2 | 4 | 0 | 0 | 5 | 0 | 1 | 3 | 0 | 1 |
| Accountants | 1 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 |
| Auditors | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Lawyers | 2 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 1 | 0 | 0 |
| Casinos | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 8 | 0 | 0 |
| Real estate | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| DPMS | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 14 | 0 | 4 | 13 | 0 | 5 | 4 | 0 | 2 | 29 | 0 | 0 | 12 | 0 | 1 | 14 | 0 | 1 |
| VASPs | | | | | | | | | | | | | | | | | | |
| VASPs | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 0 |
| Total | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

529. Banks demonstrated overall a very good understanding of the STRs reporting requirements. The table above shows that approx. 85% of all STRs are submitted by the Banking Sector. The sector has seen a significant increase (+220%) of STRs in 2020. The authorities suggest that this is the result of supervisory actions and sanctions imposed (including for non–reporting of STRs) in the sector.

166 Credit unions, Factoring and TCSPs had filed no STR over the analysed period.
167 In this table the AT refers to attempted transaction.
168 Statistics reflects on MVTS services for providing transfers via money remittances.
169 Statistics reflect on services for providing transfers via postal orders.
170 Reported suspicious transactions refer to the activity of money remittance services.

530. Banks can articulate key indicators that led to the STRs. Information provided noted that the largest number of reported STRs related to transaction accounts and internet banking. Furthermore, they explained trend analysis carried out that gave rise to typologies such as the cases where cash was withdrawn after immediately receiving a transfer into the bank account.

531. The MVTS sector (including the Croatia Post) is the second in number of STRs, after the Bank sector, with an average of 12% of all STRs. Within this sector the reporting behaviour of the MVTS service providers conducting transfer via money remittances improved, increasing as a result of higher supervisory attention and observed new typologies. With regard to postal services, the drop in the figures is explained by the supervisory authority as a result of improving the quality of the STR reporting, as previously, the recurring transactions were considered suspicious, where no other indication of illegal activity was observed.

532. The Authorised exchange offices have very passive reporting behaviour, which does not entirely match with expectations from this sector, bearing in mind the volume of an annual turnover of the sector, and exposure to cash, foreign customers etc.

533. Similarly, the Games of Chance sector had not reported any STRs until 2019. Whilst the sector is aware of the legal requirements, it was unable to articulate the controls implemented, in practice, to identify suspicious activity, nor any transactional or client trend analysis carried out. This could indicate a lack of understanding of requirements or a lack of adequate systems to identify suspicious activity.

534. Other non–Bank FIs and DNFBPs also demonstrated a good understanding of the principles of STR reporting requirements. With respect to DNFBPs, however, given the low level of STR reporting in some sectors, the knowledge was primarily theoretical. Though a lower level of reporting of STRs is expected in some sectors, there are sectors where the evaluation team consider that the level of STR reporting is too low and not commensurate with the risks. Notaries would be expected to file more STRs taking into consideration their gate–keeper role including with respect to registration of legal persons, where Croatia has systematic challenges. The real estate sector would be expected to have STRs reported, considering their market risk exposure. The accounting sector similarly would be expected to report a higher number of STRs given 1) the significantly larger number of REs, 2) this sector has been used in ML schemes due to activities it offers such as the establishment, operation or management of trusts, companies, foundations or similar legal arrangements, and 3) the client base of the sector is considered as posing a higher risk as it is estimated that 21% are non–residents and 38% are NPOs.

535. As noted in the analysis above, DNFBPs base their risk–mitigating measures primarily on pre–determined key indicators provided by supervisory authorities, and the same happens with respect to suspicious transactions. The pre–determined indicators for the detection of suspicious transactions are published by the supervisory authorities. These are not established by REs. Therefore, there is minimal effort to establish a specific and individual business risk assessment that would derive specific and individual risk–mitigating measures commensurate to their risks. In line with the inspections' findings, the indicators provided by the supervisory authorities are not always integrated into the internal controls of the DNFBPs, in a timely manner.

536. With respect to VASPs, given that this is a newly regulated sector, the AT noted that the supervisory authority is still working with the sector to ensure compliance with AML/CFT obligations. Generally, there is a considerable disparity between the VASPs understanding of their AML/CFT obligations. Nonetheless, the sector is aware of the STR reporting requirements and already filed 6 STRs in 2020.

537. REs can articulate adequate measures to avoid tipping off. However, non–Bank FI's and DNFBP's understanding was theoretical, given they have very limited examples of the submission of STRs or suspicious activity transactions. As noted above from examples observed by the AT, some REs appear to mitigate the potential risk of tipping off by filing the STR subsequent to allowing the transaction. The AT has concerns about the potential abuse of these provisions. Banks and MVTS, particularly those part of a larger or international group, have more consolidated procedures to ensure confidentiality and segregation of information to avoid tipping off.

538. In addition to STRs, all REs are required to notify cash transactions over HRK 200 000 (EUR 27 000). Notifications are to be sent in the prescribed form by mail, telefax or in another appropriate way.

**Table 5.2: Number of Cash Transaction Reports[171]**

| Reporting entities | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| Financial Institutions | | | | | | |
| Banks | 54095 | 56033 | 56375 | 57492 | 55766 | 50158 |
| Currency exchange | 488 | 441 | 513 | 550 | 541 | 454 |
| Savings Banks and Credit Unions | 350 | 385 | 292 | 358 | 317 | 341 |
| Croatian Post | 33 | 41 | 30 | 0 | 1 | 0 |
| DNFBPs | | | | | | |
| Casinos[172] | 23 | 57 | 120 | 97 | 68 | 59 |
| Notaries | 0 | 0 | 0 | 0 | 5 | 4 |
| DPMS | 0 | 0 | 0 | 0 | 0 | 1 |
| TOTAL | 54 989 | 56 957 | 57 330 | 58 497 | 56 698 | 51 017 |

539. As can be seen from the table above, 98% of all cash transaction reports are filed by Banks. Whilst this may be expected given the sector's key function in the processing of transactions, there are also other sectors that transact highly in cash and therefore there is a concern that these sectors may be underreporting, e.g., MVTS (including Croatia Post). It is understood that in the indicated sectors, the average transaction might be below the set threshold, but considering the complete absence of any reports per any giver year, this raises concerns with both: appropriate reporting above threshold transactions and ability to detect linked transactions, including the scenarios of just–below–the–threshold transactions. Supervisory authorities pay attention to the CTR reporting among the REs, but the results are yet to be achieved.

### 5.2.6. *Internal controls and legal/regulatory requirements impending implementation*

540. The legislative requirements on internal controls are quite prescriptive. All REs are aware of what their requirements are. All REs are required to implement three levels of defence against ML/TF. These include 1) documented procedures, 2) a compliance function, 3) audit function and screening and training of employees.

541. All REs are required to have an annual internal audit, annual training plan, and annual review of all its policies and procedures, however, there is no legislative requirement for having an independent audit function for all REs. Only banks and the FIs that fall under the supervision of the CFSSA are required to ensure their internal audit function is independent. Details of these

[171] MVTS, Insurance sector, Investment firms, Securities sector, E–Money, Leasing, Factoring, Real estate agents, Lawyers, Accountants, Auditors, TCSPs and VASPs filed no CTR over the analysed period.
[172] Figures include reporting by all gambling sectors.

reviews, and other information, is required to be submitted to their supervisory authority. Other than within a financial group, most REs do not outsource their AML/CFT functions.

542. Banks and MVTS that are part of a group exhibited well documented and sophisticated group–wide internal controls and procedures. These group controls and procedures also extend to other activities carried out within the group, e.g., E–Money Investment services. These sectors clearly articulated the controls implemented with respect to specific ML/TF risks identified internally, and how these are implemented, in practice. In respect to these sectors, the procedures, annual audit (including the staff training plan) are reviewed annually by the relevant supervisory authority. Banks also exhibited an understanding of the challenges when implementing internal controls, such as the fact that the sector is aware of drug trafficking risks, however, some of the banks indicated that due to the complex nature of this crime, it is difficult to detect these immediately.

543. Exchange offices, due to the nature of their activity, have simpler and less sophisticated internal controls and procedures. Nonetheless, these clearly complied with the legal and regulatory requirements, particularly focusing on controls on the use of cash. There are comprehensive requirements on the reporting of cash transactions (see. 5.2.5 above) and tighter thresholds applicable specifically to this sector to mitigate identified risks.

544. Casinos evidenced they understand their legal obligations and have documented procedures to comply with such. However, REs did not provide satisfactory information or understanding on the practical implementation of these. As noted in IO3, the lack of supervision and review of the sectors' controls and procedures brings into question the adequacy of these.

545. Smaller FI's and DNFBPs implement standard or generic procedures, focusing strictly on legislative compliance, without much consideration of the controls required to identify, mitigate, and manage ML/TF risks. Sectors such as accountants and real estate implement very basic internal controls to ensure compliance with requirements, however, these are not commensurate with their own risks and vulnerabilities.

546. VASPs are a newly regulated sector, and therefore the supervisory authorities are still in the process of providing feedback to ensure their internal controls are to the standards expected. Between VASPs, there was a considerable disparity, in the extent of implementation of internal controls. Whilst some demonstrate very technical understanding of the controls implemented, others are only able to articulate very basic controls that are not commensurate with the nature of its activities. In particular, with respect to the use of privacy coins, the sector was unable to describe what controls are implemented to manage the risks associated with such and how these complied with the legal requirements.

547. There are no secrecy laws that impede the implementation of AML/CFT measures or restrict the exchange of information between REs. REs that form part of a larger group can provide information on group–wide policies to address ML/TF risks. Most indicated the use of Group committees that consider risks and vulnerabilities and then disseminate information to the relevant subsidiaries as deemed necessary. For example, some banks noted that as part of their due diligence controls it makes use of Group resources when assessing foreign citizens, as Group could facilitate obtaining information from other jurisdictions.

### *Overall conclusions on IO.4*

548. The most important sectors in Croatia, banks and MVTS, in most instances, demonstrated sufficient application of AML/CFT preventative measures commensurate to their risks and reporting of STRs. Important sectors, such as authorised exchange, casinos and VASPs, mostly demonstrated an acceptable level of implementing preventative measures, with further major improvements required in some areas. The rest of the sectors performed weaker, but among those, lawyers and notaries displayed stronger features.

549. Understanding of ML risks and AML/CFT obligations is strongest among FI's, particularly the Bank and MVTS sectors. However, except for the Bank and MVTS sectors, there is concern about the complete lack of understanding of TF risks across all other sectors.

550. Banks and MVTS demonstrated advanced practices to application of a risk–based approach, consistent with their risk understanding and assessment of their own businesses' risks. Authorised exchange, lawyers and notaries demonstrated developing own risk indicators, and casinos, applying additional risk mitigation measures to online gambling services. The majority of other FIs apply mitigating risks uniformly, without tailoring to their risk characteristics, and confined to pre–determined criteria set out by the supervisory authorities.

551. Relatively stronger CDD performing sectors are banking, MVTS, Authorised Exchange, and online casino providers. VASPs displayed some extent of performance but need time to have measures in place at a satisfactory level. Implementation of CDD requirements to natural persons is adequate, but application of measures to identify BO of a corporate customer raises concerns within all sectors, especially when dealing with complex structures.

552. FIs, especially banks, MVTS, E–money and Payment Institutions demonstrated a higher level of effectiveness in applying EDD measures than the DNFBPs. EDD measures with respect to PEPs is an area for special attention across all sectors. Gaps in some other areas for application EDD measures are not that critically important.

553. The volume of STRs in banking and MVTS (including the Croatia Post) sectors is largely consistent with the expectations, taking into consideration the materiality and risks present in the sectors than that of the others. STR reporting in non–bank FIs, including authorised exchanges and DNFBPs, including casinos, notaries and real estate, is low and may indicate a lack of understanding of reporting requirements or inadequate controls to identify suspicious activity. Within the reporting sectors, the STRs align with the risks identified in the NRA to a large extent.

554. Bearing in mind the level of performance among the sectors having relatively more importance in Croatia's context, major improvements are still needed for IO 4.

555. **Croatia is rated as having a Moderate level of effectiveness for IO4.**

# 6. SUPERVISION

## 6.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 3***

a) All the licensing authorities and SRBs have in place legislative requirements on the prevention of criminals from holding a management function or being the BO of a REs, but among those, the CNB applies robust measures including verification of received information, while the CFSSA does so to a lesser extent. The TA and other licensing bodies apply administrative checks without verifying information on criminal background. Furthermore, there are no registration or licensing obligations for accountants, trust and company service providers, VASPs, and dealers in precious metals and stones. Although there is no systematic control of the supervised sector for detection of unlicensed operations conducted, except for in the VASP sector, adequate actions are taken to terminate unlicensed activity upon a complaint.

b) Overall, across all four supervisory authorities, the understanding of ML risks varied. The CNB and Financial Inspectorate demonstrated a comprehensive understanding of ML risks and, to a lesser degree, the CFSSA. The overall understanding of TF risk did not prove to be sufficient across all supervisory authorities, however, the CNB and Financial Inspectorate demonstrated a comparatively better sectorial risk understanding. The CFSSA places full reliance on the NRA's assessment and therefore is impacted by the deficiencies noted in IO1. The TA did not demonstrate satisfactory understanding of either ML or TF risks in the supervised sector.

c) The CNB and Financial Inspectorate have a reasonable supervisory framework, and their AML/CFT supervisory efforts are largely aligned to their understanding of the ML/TF risks. The shortcomings of risk understanding by the CFSSA and the TA also impacts the effectiveness of the supervision undertaken. In 2020 the CNB revised its supervisory cycles and approach, which is expected to make the process more risk–oriented, and resource optimised. The supervisory efforts of the Financial Inspectorate are impacted by the shortage of resources and the available IT support. The TA and the CFSSA do not have an AML/CFT specific supervisory approach, and the level of supervision is not adequate. The CFSSA, only set up its AML/CFT supervisory team in 2020, therefore, the effectiveness of this cannot be demonstrated.

d) The effectiveness and dissuasiveness of sanctions vary across the supervisors, being stronger at the CNB and Financial Inspectorate whilst weaker at the CFSSA and TA. Whilst monetary sanctions are imposed through the Council of Misdemeanour Proceedings, these are not deemed effective or dissuasive for some sectors, such as Banks. With the exception of one or two cases, other types

of sanctions are rarely or never used, such as withdrawal of individuals in management functions or withdrawal of licences.

e) Overall, there seems to be good communication and engagement between REs and supervisory authorities, with a considerable amount of guidance provided. The CNB, CFSSA and FI, carry out annual training sessions that cover items like typologies, key indicators, new trends, legislative changes, etc. This is also supported by training and engagement provided by AMLO.

***Recommended Actions***

***Immediate Outcome 3***

a) Croatia should provide all supervisory authorities with the required human resources to ensure these are adequate to permit supervisory authorities to fulfil their obligations. Vacant positions should be fulfilled by skilled professionals as a matter of urgency.

b) Croatia should implement an appropriate licensing or registration regime for VASPs, introduce a mechanism for timely identification of accountants, TCSPs and DPMS, and implement consistent market entry and on–going "fit and proper" controls for these REs.

c) The CNB should continue, and the CFSSA should enhance its efforts in applying robust market entry measures. Other licensing and registration bodies should introduce effective measures for preventing criminals and their associates from holding or being the BO of a significant or controlling interest or holding a management function when granting authorisation.

d) All authorities with licensing and registration responsibilities should implement effective tools for the identification of unauthorised operators (including where authorisation is withdrawn or surrendered) that offer (or advertise) regulated activities and conduct systematic monitoring of the market. The CFSSA should continue its systematic monitoring and identification of VASPs operating in Croatia.

e) The CNB and Financial Inspectorate should maintain and the CFSSA and TA should enhance the level of understanding of sectoral and RE – specific ML risks, and all supervisory authorities should enhance their understanding of TF risks in the supervised sectors and REs. All supervisory authorities should conduct regular assessments of the ML and TF risks in the sectors and individual REs.

f) All supervisory authorities and the Council of Misdemeanour Proceedings should review and enhance its monetary sanctions policy to ensure these are effective and dissuasive. Particularly for sectors posing a higher risk. These policies should also clearly set out when indictments are issued and how regulatory settlements may be commenced. All supervisory authorities should also apply a broader range of remedial actions and sanctions, including on individuals, in a proportionate manner.

The CNB should:

g) Review the effectiveness of its 2020 methodological procedures with respect to the inspection cycles to ensure that the level of supervisory engagement remains commensurate with the ML/TF risks identified.

h) Ensure that it applies its revised 2020 supervisory strategy and that it adheres to the supervisory cycles determined by the REs risk profile as established by its own methodology.

i) Commence the application of its 2020 methodological procedures on sectors it has to date not focused its supervisory attention, i.e., E–Money and Payment Institutions.

The Financial Inspectorate should:

j) Review the effectiveness of its 2020 methodological procedures with respect to the inspection cycles to ensure that the level of supervisory engagement is commensurate with the ML/TF risks identified.

k) Continue to enhance its IT tools to allow for the automated collation of information from REs, and faster and more effective analysis of the data.

l) Establish tighter communication with licensing bodies to ensure a timely and comprehensive handover of new REs.

The CFSSA should:

m) Strengthen its ML/TF risk assessment methodology, particularly in respect to the scope (include group–level risks), methods (describe risk scoring) and periodicity (regular and ad–hoc) of risk assessments of the supervised sector and individual REs.

n) Significantly increase its supervisory focus on RE's compliance with AML/CFT obligations and conduct on–site and off–site inspections on a risk–sensitive basis.

The TA should:

o) Develop and implement an AML/CFT methodology, and assess the ML/TF risks of the Games of Chance sector and individual REs.

p) Significantly increase its supervisory focus on RE's compliance with AML/CFT obligations. Determine on–site and off–site inspection cycles based on the results of the AML/CFT risk assessment. This should include conducting ad–hoc inspections where the risk profile of the RE changes.

q) Provide the staff with targeted training to increase understanding of: (i) ML/TF risks in the Games of Chance sector, especially in respect to risks associated with e–gaming; and (ii) its AML/CFT supervisory obligations to ensure effective AML/CFT supervision.

556. The relevant IO considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26–28, 34, 35 and elements of R.1 and 40.

## 6.2. Immediate Outcome 3 (Supervision)

557. The weighting given to the different FIs' and DNFBPs' sectors, as well as to VASPs regarding supervision, is the same as the one applied for preventive measures (see IO.4 and further details in Chapter 1). The conclusions in IO.3 are based on a wide range of information provided by Croatia on supervisory efforts and discussions with the supervisory authorities, the AMLO and LEAs, as well as interviews with a representative sample of FIs, DNFBPs and VASPs.

558. There are four AML/CFT supervisors in Croatia, supervising all REs; the CNB, the CFSSA, the Financial Inspectorate and the TA. The basic powers and responsibilities of these supervisors are set out in the AMLTFL. There are no licensing requirements currently set for accountants, TCSPs, DPMS and VASPs, but these are supervised for AML/CFT purposes by the Financial Inspectorate and the CFSSA, respectively.

559. The AML/CFT legal framework does not cover the full scope of VASPs, only applying to exchange services between virtual currencies and fiat currencies and custodian wallet providers (important sector). Nor does it cover external accountants within the scope of R.22. Hence, the supervisory efforts do not extend to these circumstances, respectively. Technical deficiencies noted within R.26–28 will have an impact on Croatia's level of effectiveness in IO.3.

### *6.2.1. Licensing, registration and controls preventing criminals and associates from entering the market*

560. Across most sectors, supervisory authorities have domestic legislative requirements and procedures to prevent criminals from holding key functions with REs. All individuals holding a key function should provide a certificate of criminal history as part of the fitness and propriety tests. Whilst this is followed, in practice, by licensing authorities, there are some deficiencies e.g., these procedures are not followed in respect to associates of criminals, and there is little verification or other due diligence carried out on individuals by the TA, MoF and sector associations.

*CNB*

561. The CNB is responsible for the licensing of Banks, Housing savings banks, Credit Unions, E–Money Institutions, Payment Institutions, and Exchange Offices. The CNB demonstrated its knowledge of business models, including corporate governance arrangement and prudential risks of licensed entities. The CNB applies robust controls when licensing REs under its remit and has clear, documented internal procedures. The principles followed for licensing by the CNB are largely the same across all sectors, however, there are some minor differences. The main difference derives from legislative requirements that establish mandatory interviews for the application to key functions to banks, whilst interviews for key functions of other sectors are only carried out if deemed necessary, e.g., if the individuals are considered as posing a higher risk. The scope of the interview is tailored to address specific risks, issues, concerns.

562. Taking into consideration that Croatia is EU Member State, specifically for Banks, the CNB also follows requirements and guidance issued by the European Central Bank (ECB). Banks that are considered as systemically important, and that fall within the criteria of the ECB either as a 'significant bank' (SI) or a 'less significant bank' (LSI)[173], the CNB will liaise with the ECB to

[173] https://www.bankingsupervision.europa.eu/banking/list/criteria/html/index.en.html

provide joint approval to these applications. With respect to the approval of individuals holding a key function within a SI or LSI, the ECB is also invited to attend the interviews.

563. As part of the licensing process, the CNB comprehensively analyses information provided by the applicants. Applicants are required to provide information on individuals or corporates holding key functions, i.e., management and supervisory boards, shareholders and all BOs holding over 10% (or 25% in the case of exchange offices). The relevant sectorial acts are satisfactorily prescriptive in establishing the information required to be provided by applicants, including the need to provide evidence of the absence of criminal record history (criminal investigations or convictions) on any of these individuals. The CNB applies comprehensive fitness and propriety tests on shareholders and BOs that includes the verification of the information with a wide range of external sources. The prohibition of the approval of individuals with a criminal background is absolute and appropriately prescribed in the sectorial legislation, which is also reflected in the CNB's internal documentation and is aligned with the FATF Standards. CNB measures also include suitable albeit basic due diligence (primarily open–source checks) on associates of the applicant to identify any potential association to criminal activity.

564. It is, however, observed that there is a gap in a set communication mechanism between LEAs and the CNB (as well as other licensing authorities), which can undermine the CNB's efforts in applying preventative measures. If whilst authorised by the CNB, such a subject appears within the attention of LEAs, including when charged or convicted, the CNB would not be informed proactively. This would rather be detected at the stage of monitoring or assessment of the entity by the CNB (see also IO.1).

565. Source of funds is also a key component of applications. The CNB will request detailed and extensive information and evidence of the source of funds of the acquirer of shares in a FI that allows it to make an appropriate and informed decision. This would include considering financial arrangements with other BO of the applicant or other RE. An example was provided when the source of funding was a bank loan, where the CNB requested exhaustive information and analysed the loan agreement in detail.

566. The approval to the management or supervisory boards for some sectors is provided for a defined time (e.g., Credit Institutions management board – 5 years, Credit Institutions supervisory board – 4 years, Credit Union management and supervisory boards – 4 years). Upon completion of the time, the individual will have to reapply to continue to carry out the key function. Furthermore, changes in ownership or key functions for all sectors also require notification to the CNB. The CNB will apply the same fitness and propriety due diligence scrutiny on any applicants regardless of if new to the market or existing authorised individuals. REs are also required to submit annual information on approved persons to confirm no changes to the condition of their approval. This includes confirmation of no criminal investigations or convictions. With respect to the annual submissions on key function holders, the CNB relies on the data provided by the REs and does not verify if adverse information is received or identified.

567. The table below depicts in further detail the applications approved, withdrawn, and refused by the CNB. As can be seen, the number of new entrants (with the exception of exchange offices) is very low and therefore, the potential number of refusals is low.

**Table 6.1: No. of applications and licence surrenders (2015–2020)**

| Type of entity | Number of applications approved | Number of applications withdrawn | Number of applications rejected | Number of licenses withdrawn voluntarily |
|---|---|---|---|---|
| Banks | 0 | 0 | 1 | 10 |
| Housing savings banks | 0 | 0 | 0 | 0 |
| Credit unions | 1 | 0 | 1 | 10 |
| Exchange offices | 342 | 20 | 3 | 466 |
| Payment Institutions | 4 | 1 | 0 | 1 |
| E–Money Institutions | 2 | 0 | 0 | 2 |

568. The CNB rejected 1 application where a foreign national applied for acquiring an existing Bank where it was impossible to verify the source of funds for acquisition and the business plan indicated at a very high AML/CFT risk appetite. See the further details in the case below.

**Box N°6.1: Rejected Application**

The CNB received an application by foreign nationals to acquire an existing Bank.

The CNB's analysis and checks established that no proof was submitted on the availability of the funds, with discrepancies on the actual figures identified between various documents. Furthermore, the business plan submitted was considered to be unrealistic, with an extremely high growth rate that the applicants could not justify. Checks carried out with foreign authorities also identified that the applicants had been part of another RE whose authorisation had been revoked by the relevant supervisory authority due to a highly risky credit policy, insufficient placement provisions and inadequate AML/CFT controls.

Therefore, the CNB assessed that none of the BO's met the legal criteria of suitability and financial condition, with the result that the application for prior approval to acquire a qualifying holding in a Bank was rejected. The AMLO was notified of this decision.

569. On one occasion, the application for a credit union was rejected for the reason of presenting untrue and incorrect information, as presented in the case below.

**Box N°6.2: Rejected Application**

The CNB received an application for the authorisation of a credit union, including the individuals proposed for the management board.

The applicant's financials were assessed as inadequate and unrealistic for a number of reasons, such as unsupported explanations for the significant increase in deposits, underestimated loan value adjustments, overestimated the increase in interest income, and questionable business sustainability.

Furthermore, as part of the fit and proper process of the individuals holding key functions, it was identified that the information contained in the application questionnaire for one member of the management board was untrue and incorrect. The applicant has omitted information about bankruptcy proceedings of a previous employment.

Therefore, the CNB's final decision was to reject the application.

570. There were 10 Banks and 10 Credit Unions that entered into bankruptcy, voluntary wind down proceedings, or a merger, and in these cases, the RE's authorisation will automatically lapse. With respect to the bankruptcy proceedings, the court appoints a bankruptcy administrator to monitor the activities of the RE during the process, whilst in respect to voluntary wind down proceedings, the CNB will monitor the RE adherence to the previously agreed wind–down plan. Croatia authorities observed that the reason for the number of firms under bankruptcy, voluntary wind–down proceedings or mergers, is primarily due to changes in the economic situation of the country. There is, however, one case that has been part of a criminal investigation for over 10 years.

571. With regards to the 3 rejected applications for exchange office, in each case, it was established that a criminal offence was committed. A total of 562 exchange office licences were withdrawn during 2015–2020. 18 of them were revoked due to criminal offences or misdemeanours for which judgements with final force and effect were passed, and the remainder due to other non–criminal reasons.

572. The e–money and payment institutions' licences were withdrawn at the request of the firm.

573. The CNB does not carry out any checks or follow up actions to determine that an entity has stopped its activities following the withdrawal of an application or surrender of its authorisation.

574. The CNB noted that when applications are rejected, it does not inform other domestic competent authorities of adverse findings. Hence, the individuals may apply to be authorised for any other activity under any of the other licensing or supervisory authorities.

575. With respect to unauthorised activity, the CNB does not have written procedures in place to identify unlicensed operators, nor does it have measures in place to identify these. Cases of operators providing a regulated activity without authorisation are identified when third–party information is received, e.g., through complaints. Once information is received, the CNB does effectively deal with potential unlicensed operators, and will publish warnings on its website to dissuade the continuation of those services and raise awareness to customers. However, the CNB does not record any statistics or information on any cases of unlicensed operators identified and on which it has taken action against. The lack of procedures and systematic action on unlicensed operators raises a plausible vulnerability in Croatia's supervisory regime and potentially exposes the financial services market to abuse by criminals.

**Box N°6.3: Unlicensed Payment Institution**

In 2015 the CNB received a passporting notification from the UK Financial Conduct Authority, notifying that E–Money Institution "A" wished to provide E–Money and payment services in Croatia, as per the passporting services of the E–Money Services Directive.

The CNB received information that two Croatian based companies were advertising as being representatives of E–Money Institution "A" and were offering payment card contracts. The CNB contacted the UK FCA, who confirmed that these companies were not associated to E–Money Institution "A".

The CNB proceeded to issue a public warning about these entities on its website.

*CFSSA*

576. The CFSSA is responsible for the registration of VASPs and the licensing of life insurance companies, investment fund management companies, pensions companies managing voluntary pension funds, pension insurance companies, investment firms, leasing companies, and factoring companies.

577. The CFSSA noted that a licensing regime had not been implemented for VASPs as it was not a requirement of the EU 5th AMLD. VASPs set up in Croatia are required to notify the CFSSA about their activities within 30 days after launching their activities or registering the legal person. Hence, there are no checks done to ascertain the fitness and propriety of the individuals associated with VASPs, or their associates. At the time of the on–site visit, there were 15 VASPs registered with the CFSSA. In the light of growing interest in this activity and increasing materiality of the sector in Croatia[174], the assessment team considers that the current measures in place are not adequate. On a positive note, the recent steps taken by Croatia suggest authorities' willingness to progressively improve the situation. Furthermore, the registration requirement falls short of the FATF Standards because of the limited scope of activities under the definition of the VASPs.

578. In order to support its licensing process, the CFSSA is using a wide range of sources and co–operation to gather information required to analyse the application. The CFSSA also liaises with foreign supervisory authorities where necessary. Whilst there are legal provisions that establish the statutory gateways for the exchange of information with foreign competent authorities, there are no established internal procedures. Overall, between 2018–2019 there have been 35 requests sent to foreign counterparts, focusing on fit and proper matters. Issues with the timely exchange between the LEAs and the licensing authorities on authorised persons are relevant also for the CFSSA.

579. When licensing FIs, the CFSSA has a comprehensive checklist that it uses when processing applications for all sectors. The checklist contains items relating to the fitness and properness of authorised persons (management board, supervisory board, shareholders and BOs with a threshold over 10%). Documents requested, as prescribed in the relevant sectorial laws and as aligned with FATF Standards, include, among others, an adequacy assessment of the individual made by the firm. Each individual holding a key function is also required to prove the absence of criminal records, including providing a certificate from the MoJA. In relation to foreign citizens, the criminal background certificate is required to be not older than 3 months and notarised by the relevant competent authority of the previous jurisdiction in which he/she was resident. This information is verified against a range of domestic and foreign sources, specifically in respect to ensuring that the applicant does not have a criminal background.

580. The consideration of the application includes an assessment of whether the applicants associated with criminals. Similarly, criminal records are requested for associates of key function holders, and basic due diligence is conducted on them. The sectorial legislations are also satisfactorily prescriptive in absolutely prohibiting the approval of individuals with a criminal background, which is also reflected in the CFSSA's internal documentation and is aligned with the FATF Standards.

[174] https://coinatmradar.com/bitcoin–atm–near–me/

**Box N°6.4: Due Diligence on criminal associates**

In 2019 and 2020, the CFSSA received an application by two individuals to acquire an existing insurance company. The CFSSA requested criminal records of the two proposed acquirers. Furthermore, it also requested criminal records, i.e., official certificates issued by the home countries and not older than 3 months, of their associates. This amounted to receiving information on the criminal background of 50 other individuals.

581. The CFSSA also noted that it introduced a list of natural persons that have been previously engaged in illicit activities within the capital market sectors and that it closely monitors their activities. However, to note that the AT has not seen this list or how it is used as part of the CFSSA's supervisory efforts. Furthermore, no information is requested or checks done on the source of funds or wealth of new applicants.

582. The table below notes the applications approved, withdrawn, and refused by the CFSSA. The CFSSA does process a significant number of applications, however, there have been no rejections, and this could indicate that the diligence carried out on applicants is not robust enough to identify fit and proper issues.

**Table 6.2: No. of applications and licences (2015–2020)**

| Type of entity | No. of Management Board Member approvals | No. of application approved | No. of applications for change of control | No. of withdrawn applications | No. of rejections | No. of licence surrenders |
|---|---|---|---|---|---|---|
| Life Insurance companies | 64 | 0 | 13 | 28 | 0 | 0 |
| Investment funds management companies | 93 | 9 | 31 | 2 | 0 | 1 |
| Pension companies managing voluntary pension funds | 28 | 0 | 0 | 0 | 0 | 0 |
| Pension insurance companies | 6 | 1 | 1 | 1 | 0 | 0 |
| Investment firms | 17 | 0 | 1 | 1 | 0 | 1 |
| Leasing companies | 71 | 0 | 37 | 0 | 0 | 2 |
| Factoring companies | 34 | 13 | 23 | 1 | 0 | 0 |

583. The CFSSA does not carry out any checks or follow up actions to determine that an entity has stopped its activities following the withdrawal of an application or surrender of its authorisation.

584. With respect to unauthorised activity, the CFSSA does not have written procedures in place to identify unlicensed operators. Despite this, the CFSSA demonstrated to make efforts in identifying unlicensed and unregistered entities, focusing more on the detection of VASPs operating in the market. The CFSSA has evidenced that it actively monitors the market through public information such as social media to identify unregistered VASPs operating in Croatia. The CFSSA has been contacting VASPs identified to ensure they formally notify the CFSSA of the services provided, etc.

585. On the basis of the following example, it was observed that there is a gap in knowledge as to what constitutes the VASP activity. The AT identified that the Croatian Post advertises on its

website the exchange of virtual assets for FIAT, however, it is not notified as a VASP. The CFSSA advised that the Croatian Post would not be required to register given that the Croatian Post acts like an "intermediary" as the services are provided on behalf of another registered VASP. This is questioned by the AT because: (1) the advertising clearly noted the Croatian Post as providing an exchange of virtual assets and FIAT as defined within the AMLTFL; and (2) the AMLTFL does not provide for "intermediaries" or "agents" of VASPs. Hence there appears to be a gap in regulation here, and there could be other REs potentially carrying on VASP activity without registration.

586. With respect to other types of unlicensed operators, the CFSSA demonstrated in most cases to get information from third parties, e.g., through complaints. When information is received about a potential unlicensed operator, the CFSSA adequately investigates the matter to determine whether the operator is providing regulated activities, and it takes action. There have been 5 cases investigated in the evaluated period with public notices issued in respect to investment entities in all cases.

587. In addition, the CFSSA advised conducting analyses of legal persons registered with the Court Register to identify the ones that provide services to be licensed without authorisation from the CFSSA. As a result, there was 1 unlicensed company detected providing leasing services. The CFSSA conducted an investigation and issued a public prohibition order on the firm (see case below).

**Box N°6.5: Unlicensed Leasing company**

In 2019, the CFSSA identified that a company was registered with the Court Register as providing leasing activity, without approval from the CFSSA. The CFSSA investigated the matter and contacted the firm requesting further information to determine potential unlicensed activity.

The investigation concluded that the Company had entered into 3 leasing contracts and at the request of the client, acquired vehicles in such a way that by purchasing from the supplier, the Company acquired ownership of those vehicles and gave them to its customers for use.

The Company was obliged to de–register the leasing activities from the Court Register because it did not meet the conditions for performing the leasing activity, and accordingly, it was prohibited from carrying on such activities.

The CFSSA also published its decision on its website.

*Tax Administration – Games of Chance*

588. The licensing process followed was described by the TA as an administrative process. Therefore, it focuses solely on ensuring that all relevant documents prescribed by the relevant legal provisions have been submitted. There are no due diligence checks nor is a risk–based approach applied. Once a complete application is confirmed by the TA, proposals for granting authorisation are then made by the TA to the MoF for final decision. As prescribed by the MoF, only a set amount of licences can be granted for games of chance, i.e., 20 for casinos, 20 for betting entities and 50 for slot machines.

589. Casino applicants must provide proof of no criminal record for the authorised persons (director, founders of the company, beneficial owners, supervisory board members). Foreign citizens are required to provide an appropriate certificate from the domicile state and a certificate from the state in which they resided for the last two years prior to the application. No further due diligence is carried out to verify the data received or assess the potential ML/TF risks of the

applicants. Furthermore, there are no clear policies or procedures to capture associates of criminals entering this sector.

590. Any changes of authorised persons would follow the same administrative process as described for registration of a Casino. Similarly, there are no ongoing criminal checks done on key function holders or BOs of Casinos. The issue of lack of proactive or timely communication of information by LEAs on authorised persons and BOs is also relevant here.

591. With respect to unlicensed operators, in spite of not having any documented procedures, in practice the TA is more pro–active in identifying these than other supervisory authorities. The TA advised that between 2015–2021[175], it had addressed 117 illegal operators and blocked 477 IP addresses of webpages claiming to provide games of chance in Croatia. By the same means, the TA can also identify if an operator that surrendered its authorisation, or had its authorisation withdrawn, had continued to provide services without authorisation. However, no information has been provided on the process followed to identify these cases.

*Other*

592. Some DNFBPs are licensed/registered by the MoF or sector association group. These include: (i) Lawyers – Croatian Bar Association; (ii) Notaries Public – Croatian Notaries Chamber; (iii) Tax Advisors – Croatian Association of Tax advisors; (iv) Real Estate Brokers – Croatian Chamber of Commerce, and (v) Auditors – MoF.

593. The process followed by the MoF and the four associations is largely similar and as prescribed by law. The process is very much an administrative task that focuses solely on ensuring that all the relevant documents as prescribed by the relevant acts are submitted. Applicants must evidence the absence of a criminal record by providing copies of criminal certificates. In cases where the RE had not resided in Croatia for long, criminal records of his/her previous place of residency are required. The period for the criminal record certificate ranged from 5 to 10 years.

594. There are no other due diligence checks carried out on the applicant REs, key function holders, or BOs, to assess potential ML/TF risks or verify the information received. Furthermore, there are no clear policies or procedures to capture associates of criminals entering these sectors.

595. No ongoing due diligence is carried out on authorised REs, however, if adverse information is identified or received, then action can be taken to withdraw the RE's authorisation. The MoF and sector associations will rely on the REs obligation to notify if they are subject to an investigation or criminal conviction. There is no sharing of information between associations, supervisory authorities or law enforcement agencies. E.g., the Croatian Association of Tax Advisors provided an example about an RE that notified the association that he was subject to a criminal investigation. The RE made the notification when the case was published in the media. The Croatian Association of Tax Advisors did not receive any information from the Financial Inspectorate, as the supervisory authority, or LEAs that were carrying out the investigation.

596. The Croatian Bar Association provided various examples of individuals that had been withdrawn from their register, however, these were primarily due to disciplinary procedures in respect to their conduct, ethics or professional advice, and not criminal offences.

[175] Year 2021 refers to the period before the end of the on–site visit.

*Non–Licensed/Registered*

597. There are no licensing, registration or other measures to prevent criminals and associates of criminals from entering the following sectors – Accountants, DPMS, and the TCSPs, despite the sectors, are not assessed as having proven low level of ML/TF risks.

598. During the on–site, it was noted that the Financial Inspectorate had proposed to establish a licensing regime for accountants because it considered that it would improve the transparency and supervision of the sector and allow better management and mitigation of ML/TF risks in the sector. The lack of licensing regime gives rise to challenges and issues, such as difficulty in supervising as there is no clear register to know which entities are carrying on the activity; or delays in identifying potential risks and non–compliance given there is no market entry requirements or scrutiny. However, the proposal had not been accepted. The reasons for such ranged from pressure from the accounting industry that objected to further regulation, lack of resources, to ensure commercial competitiveness with other EU jurisdictions, or because the European Council had not permitted it. Ultimately, the Financial Inspectorate's proposal was rejected by the working group for drafting Accounting Law.

599. With respect to DPMS, there appears to be a misunderstanding by the Croatian authorities of the FATF Standards. The Financial Inspectorate noted that DPMS are not caught under the FATF Standards given they are prohibited from transacting in cash above EUR 10 000. This assumption seems to be based on the FATF R.22(c.22.1(c)) and R.23(c.23.1(b)), which specifically require DPMS to apply CDD and STR controls only when they engage in any cash transaction with a customer equal to or above USD/EUR 15 000. However, DPMS are not exempt from other FATF requirements, such as the appointment of a licensing body to prevent criminals from entering the market and a supervisory body to monitor compliance with other FATF Standards.

600. No specific consideration was given to licensing of the TCSP sector.

### *6.2.2. Supervisors' understanding and identification of ML/TF risks*

601. Overall, across all four supervisory authorities, the understanding of ML risks varied, the strongest being demonstrated by the CNB and weakest by the TA. With respect to TF risks, the overall understanding did not prove to be sufficient across all supervisory authorities, however, the CNB and Financial Inspectorate demonstrated a comparatively better sectorial risk understanding. Both had carried out suitable analyses to assess the TF risks in certain areas, e.g., transactions to higher–risk countries. The CFSSA and TA place full reliance on the NRA's assessment that there is low TF risk in Croatia and hence do not seem to place any focus on this area. However, there are sectors and activities that warrant the need for greater emphasis to ensure that TF risks are identified, mitigated and managed, e.g., E–money institutions, payment institutions and VASPs.

*CNB*

602. The CNB demonstrated a very comprehensive understanding of the ML risks and a basic understanding of TF risks of the sectors it supervises. This risk understanding was developed through the combination of its ongoing supervision, assessment of the risks in the sectors, and individual RE risk profiling, the outcomes of the NRA and the EU risk assessments. The main risks/vulnerabilities observed were the potential misuse of cash, risks associated with non–resident customers, private banking products inherently carrying a greater risk due to the

characteristics, transactions to or from higher–risk countries, or the need for REs to further enhance their CDD in respect to the customer identification and verification or BOs.

603. The CNB classifies the supervised sectors and the individual REs into four risk categories and applies respective supervisory attention to the sectors, including on–site and off–site supervisory tools accordingly. The sectorial ML/TF risk assessment for Banks is carried out annually whilst the other sectors, credit unions, house savings banks, E–Money Institutions and Payment Institutions, are assessed every 2 years.

604. Extensive and comprehensive qualitative and quantitative data is collected by analysing relevant annual regulatory reports submitted by all REs and other data available to the CNB, including data obtained through the annual questionnaire submitted by REs. Qualitative information is collected from external sources, findings from previous on–site inspections, and other information collated as part of the CNB's supervisory duties.

605. The CNB has established a comprehensive analytical methodology for the assessment of all factors, providing risk scores for each risk category, i.e., country, geographical, product/service, and distribution channels. Subsequently, control mechanisms are considered to finalise and produce a residual risk assessment. Specifically for banks (excluding savings banks and credit unions), group risks are also considered, including the group activities, countries trading, etc. The CNB has evidenced that all Banks have been assessed against the revised analytical methodology, resulting in an overall risk score reflective of the Bank's inherent risks based on the relevant business model, client base, and Bank activities.

606. All risk assessments are completed with a comprehensive report setting out the scope of the review, the methodology applied, findings, recommendations and actions taken. The sectorial risk assessment samples were very comprehensive and considered qualitative and quantitative data resulting in inherent risk analysis and residual risk analysis.

*CFSSA*

607. The CFSSA risk understanding was confined to the findings of the NRA. Respectively, the CFSSA could demonstrate adequate knowledge of ML risks of its sectors, but the TF risk understanding was affected by the quality of the NRA (see IO.1). The CFSSA noted that the main risks/vulnerabilities observed in the supervised sectors were as described within the NRA, such as the need for continued education and training of RE employees on their obligations and risk exposures, broker scams, or the use of privacy or anonymous products within the VASP sector specifically.

608. In 2020, the CFSSA set up its AML/CFT supervision team, for which it should be commended. Prior to 2020, the AML/CFT supervision was conducted within the scope of the prudential supervision framework and thus was not ML/TF risk–based. It is, therefore, still premature to fully assess the effectiveness of the CFSSA's understanding and controls in the scope of its new setup.

609. Qualitative and quantitative data is submitted periodically by REs. The data collated is used to carry out annual assessments of each RE, assess the possible impact of REs on the financial stability of the market in which it operates, and support the CFSSA's own understanding of the sectoral risks. However, it was not evident what is the scope of this data collation exercise, the analytics carried out, whether the analyses consider the Group risks, what are the results of this, etc.

610. When discussing the scoring of the sectorial risks, the CFSSA relied on the NRA findings. It should be noted that risk scoring data provided on individual REs demonstrated that all REs within the same sector had been assigned the same risk score as the sector NRA score, regardless of their size or type, etc. The reason for this approach is that the CFSSA has not yet assessed its REs in respect to ML/TF risks.

611. The CFSSA has well documented internal Rules of Procedures that set out how REs are risk assessed. The risk assessment is carried out in six steps 1) collection of RE specific data, 2) sector–wide risk factor analysis, 3) analysis and assessment of risk factors at the level of the supervised entity to which it is exposed or may be exposed, 4) analysis and assessment of control mechanisms that reduce the risks, 5) determining the risk profile, and 6) ongoing supervision and follow up. In addition, it has developed an internal guidance note aimed to assist staff when carrying out the supervision of the securities sector, however, there is nothing similar for other sectors.

612. Even though quantitative data is collated, the risk profile is subjective to the individual carrying out the assessment, and the guidance offered is limited to a list of four categories of ratings with a vague definition, e.g., "1 – Low risk– RE is very likely not to be at risk[176]".Without a more specific and comprehensive risk assessment approach, there is a potential risk that firms will not be scored adequately, and this may also lead to a lack of consistency across REs and sectors.

613. The CFSSA considers that overall, the sectors under its supervision pose a lower ML/TF risk in comparison to other sectors because: (1) they practically do not use cash; (2) they are small in size compared to the Croatian market, and (3) the nature of the services. However, no analysis or other information was provided to evidence the basis of these views. Whilst this conclusion could be acceptable in respect to the cashless activities, it is questionable on what basis such conclusions have been made considering that the CFSSA supervises investment firms, funds related entities and VASPs, three sectors that will generally provide multi–jurisdictional activities.

614. The CFSSA demonstrated a positive approach in constructing a sectorial assessment of the vulnerabilities of the VASP sector because this sector is newly regulated and was not captured by the 2020 NRA. The assessment is a satisfactory first attempt – its scope covers data from REs on transactions, composition of the organisation, activities, and information supplied, and analysis carried out by AMLO and other LEAs. It also demonstrates Croatia's ongoing approach to developing its risk understanding of the sector, such as the identification of the use of privacy coins (e.g., Monero) by some VASPs which could pose a significant ML/TF risk and risk of abuse by criminals and is contrary to the legal provision in the AMLTFL. Although there are some limitations to note, e.g., not all VASPs may have been captured given the lack of registration requirements for this sector, and the assessment did not produce any action points.

*Financial Inspectorate*

615. The Financial Inspectorate demonstrated a very comprehensive understanding of the ML risks of the sectors it supervises. TF risk understanding was adequate for sectors with a higher level of supervisory attention, such as MVTS, exchange offices, and accountants.

[176] Other scorings are defined as: 2 – "Medium low – RE is unlikely to be at risk"; 3– "Medium high – RE is likely to be at risk"; 4 – "High risk – RE is very likely to be at risk".

616. It may be concluded that the Financial Inspectorate's understanding of risks was wider than the results of the NRA. The Financial Inspectorate uses a range of factors, including the NRA, EU NRA, results of ongoing supervision, and firm–specific assessments when determining its supervisory measures. E.g., analyse the use of money remittance by FTFs, through social media. Whilst the majority of its sectors have been assigned the same vulnerability score within the NRA at a level of medium, except for the MVTS sector scored at a level of Medium–high, the Financial Inspectorate's sectoral risk analysis scores were slightly different, and sometimes stricter (e.g., Accountants and the DPMS). This is mostly because the NRA grouped some sectors (DNFBP) together, whereas the Financial Inspectorate took a more granular, sector–specific approach. The primary focus of the Financial Inspectorate is on MVTS and accountants, given concerns on the vulnerability of these sectors and their materiality. The sectorial risk assessment samples were very comprehensive and considered qualitative and quantitative data resulting in inherent and residual risk analysis.

617. The Financial Inspectorate demonstrated a very good understanding of the risks of the MVTS sector. It was able to articulate the vulnerabilities identified within the sector and hence had driven more intensive supervision of these REs. For this sector, the TF risk was assessed separately for two sub–sectors: for the money remittance transfers, which was assessed as medium–low TF risk, and for money transfers via postal orders, which was assessed as low TF risk. The TF sectorial assessment included information on international assessments such as the EU Supranational risk assessment and the 2020 Report of the SIA. It also included an inherent risk assessment that captured extensive data on customers activities and inflows and outflows of transfers. Lastly, a residual risk assessment was documented that captured the AML/CFT measures implemented by the sectors. The assessment concluded with a series of risk mitigation action points such as a more intensive on–site approach to verify controls implemented by REs and further training offered to the sector. Furthermore, the Financial Inspectorate provided the AMLO and the MoI with three comprehensive notices related to human trafficking or TF, identified as part of the analysis conducted.

618. In respect to accountants and authorised exchanges, the Financial Inspectorate acknowledged vulnerabilities identified in recent years within these sectors, e.g., accountants associated with typologies published by AMLO and potential abuse by criminals, and the cash intensive use of exchange offices.

619. The Financial Inspectorate uses a well–documented methodological manual when assessing the REs, which is setting the practical application of a risk assessment. Guidance is also provided to the team on what factors to consider when determining the risk score. This includes analysis and evaluation of: (i) RE's products, services, transactions; (ii) the structure of the customers, including the size of the customer base, and the exposure to higher risk customers; (iii) geographical areas of activity, including the assessment of inflow/outflows of funds; and (iv) delivery channels such as non–face to face or the use of introducers.

620. To note that the Financial Inspectorate faces an added challenge given that it is not responsible for the licensing of any of its REs. With respect to Exchange Offices and MVTS that are authorised by the CNB, the Financial Inspectorate has demonstrated a good relationship with the CNB and orderly handover of new REs in these sectors. However, the same cannot be said for the other sectors. Other REs authorised by the MoF, sector bodies or sector associations do not notify the Financial Inspectorate of new licensees at the time of authorisation. The Financial Inspectorate will annually obtain a list of companies trading within these sectors from the Court Register or from the relevant licensing bodies. Furthermore, the Financial Inspectorate is

responsible for accountants, DPMS and TCSPs, that do not require authorisation. Similarly, it will obtain a list of firms trading within these sectors from the Court Register. However, there is clearly a gap of information here and potential vulnerability because there is a period of delay between when REs are licensed and the annual checks carried out by the Financial Inspectorate to identify these, and because there is no handover of information from the licensing authorities on the type and volume of activity, BOs, key function holders, etc. This will impact its supervisory assessment and, ultimately, its understanding of the ML/TF risks of the individual REs and overall sectors.

621. All REs under the supervision of the Financial Inspectorate are required to submit annual questionnaires that collate extensive information on the RE's type of products/services, client base, etc. This information supports its sectorial and individual RE risk assessment. The annual questionnaires in turn, appeared to be very extensive and inclusive. The questionnaire collates qualitative and quantitative data based on an around initial 600 possible questions. The questionnaire is then tailored to the specific characteristics of a sector or RE to ensure that the data collated is relevant. Note that the collation and assessment of these annual questionnaire is resource intensive and is all done manually. There has been some automation done in recent years, however, the AT considers that further automation and improvements to its IT systems would allow for faster and more effective assessment of the data collated. This, in turn, may free resources needed for other supervisory obligations. These improvements are part of the NRA's Action Plan and are expected to happen before the end of 2021.

*Tax Administration*

622. The TA was unable to adequately articulate its understanding of the ML/TF risks of the games of chance sector. The knowledge was limited to that contained within the NRA. It is likely that this is a result of the fact that the TA carries out "indirect" supervision of the sector only. Supervision of AML/CFT systems of controls and compliance is only done as an additional function to the tax audits carried out by the TA. (See 6.2.3 below for more information)

623. The TA has not demonstrated that it carries out any internal assessments to corroborate, monitor or identify ML/TF risks within the Games of Chance Sector.

### *6.2.3. Risk–based supervision of compliance with AML/CFT requirements*

624. The CNB and Financial Inspectorate have a reasonable supervisory framework, and their AML/CFT supervisory efforts are largely aligned to their understanding of the ML/TF risks. The shortcomings of risk understanding mentioned in the section above have an impact on the risk–sensitive supervision undertaken by the CFSSA and the TA. The CFSSA only set up its AML/CFT supervisory team in 2020, therefore it is very premature to be able to assess its effectiveness, and the TA does not have an AML/CFT specific supervisory approach.

*CNB*

625. The CNB has a reasonable AML/CFT supervisory framework that takes into account the REs' risks.

626. The CNB has a dedicated unit with responsibility for the AML/CFT supervision of all its sectors. The AML/CFT Supervision organisational unit is comprised of 9 individuals, with 3 vacant positions at the time of the on–site. They hold responsibility for approx. 53 REs, including

23 Banks[177]. The vacancies arose from the 2020 NRA Action Plan. The CNB advised that additional staff is required to ensure implementation of the new supervisory strategy, and that fulfilling the 3 vacant positions was an ongoing process during the on–site. The AT recognises the experience and knowledge demonstrated by the CNB employees, and their dedication to achieving their objectives.

627. The framework combines on–site and off–site measures with different intensities, in addition to outreach activities. The CNB revised its supervisory cycles in 2020. The frequency of routine on–site inspections currently ranges: for banks, credit unions, and house savings banks[178] – from two years for the High risk category to as necessary for the Low risk category; for E–Money Institutions[179] and for Payment Institutions[180] – from three years for the High risk category to as necessary for the Low risk category, with a different timeline for the Medium risk categories. These on–site inspections are also supplemented with periodic meetings between the cycles and annual reports for all the sectors.

628. Previously, the cycles were shorter in respect to medium high and medium low risk banks and savings banks, but these were not always adhered to, partly due to insufficient resources. The credit unions, E–money and payment institutions did not have any predetermined cycles, and on–sites would be considered only as necessary regardless of the risk posed by the RE. Within the last five years, the CNB has focused its on–site supervision on the Banks (not including Housing Savings Banks or Credit Unions). However, prior to 2020, the supervisory cycles were not always adhered to. The supervisory cycles were established by the CNB based on its understanding of the risks posed by the specific RE, therefore, not following the periodic on–site cycles on banks has potentially given rise to risk exposure during 2015–2019. Furthermore, there has not been active on–site supervision on the other sectors it has responsibility for, i.e., E–money and payment institutions since 2016.

629. The CNB revised its supervisory cycles following the analysis of the past practices and the sectoral risk assessments. When deciding on the supervisory order and intensity at the REs within the sector, the CNB takes into consideration the ML/TF risk scoring of an individual entity. It was concluded that higher intensity assessments with lower coverage are more effective. This allows for resources to focus on the highest risk REs. The CNB can be commended for implementing a more proactive supervisory approach on higher risk sectors.

**Table 6.3: Number of on–site supervision (2016–2020)**

| | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **REs** | **On (off)–sites** | **REs** | **On (off)–sites** | **REs** | **On (off)–sites** | **REs** | **On (off)–sites** | **REs** | **On (off)–sites** |
| Banks | 26 | 5(33) | 25 | 5(31) | 21 | 5(27) | 20 | 4(25) | 20 | 0(30) |
| Housing savings banks | 5 | 0(5) | 5 | 0(5) | 4 | 0(4) | 3 | 0(3) | 3 | 0(3) |
| Credit unions | 23 | 0(23) | 21 | 0(21) | 20 | 0(20) | 21 | 0(21) | 19 | 0(19) |
| E–Money Institutions | 5 | 1(6) | 5 | 0(6) | 5 | 0(5) | 5 | 0(5) | 5 | 0(5) |

[177] Banks and Housing savings banks.
[178] High risk – 2 year, Medium–high risk – 4 years, Medium–low risk – 6 years, Low risk – as necessary.
[179] High risk – 3 year, Medium–high risk – 5 years, Medium–low risk – 6 years, Low risk – as necessary.
[180] High risk – 3 year, Medium–high risk – 5 years, Medium–low risk – 7 years, Low risk – as necessary.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Payment Institutions | 2 | N/A[181] | 3 | N/A | 3 | 0(3) | 3 | 0(3) | 3 | 0(3) |

630. The CNB also carries out periodic off–site supervision on all REs as per its methodology. The off–site supervision is to a large extent aligned to on–site supervision, including a full review of all policies and procedures, review of transaction data and client files. The off–site risk assessment reports evidenced that this is a comprehensive process, on par with the on–site assessments conducted. The decision to opt for on–site or off–site supervision is primarily driven by the need to limit the impact on resources, thus limiting the number the employees and the time spent out of the office at any given time. Off–site supervision will also result in feedback provided to firms setting out remediation plans, and where necessary, the submission of indictment for any breaches identified.

631. Furthermore, REs are required to annually submit a set of documents consisting of a questionnaire, training plans, and external and internal audit reports. The questionnaire also collates qualitative and quantitative data that feeds into the annual risk assessment of each RE. Therefore, in effect, all REs are risk assessed annually. The combination of on–site and off–site supervision, in addition to the periodic collation of qualitative and quantitative data, demonstrates the CNB's effectiveness of supervision.

632. In 2018, the CNB commenced a new supervisory approach that focuses on thematic on–site reviews. Previously full scope on–sites would be carried out to review and verify all aspects of AML/CFT obligations. Since 2018, the CNB has solely focused on 3 main areas; beneficial ownership, non–resident customers and private banking customers, which are areas identified within the NRA as posing a higher risk to Croatia. The new approach of thematic reviews commenced in 2018 is considered more of deep–dive reviews, comprehensively scrutinising and challenging the controls implemented by the Banks. The CNB can be commended for implementing this new approach which has demonstrated to be more effective.

633. In 2019, the CNB identified a significant number of failings within one of its largest Banks. The on–site was driven due to various factors; the commencement of the new thematic review focusing on areas identified within the NRA as posing a higher risk to Croatia, a typology published by AMLO in respect to non–resident customers and follow up from the previous on–site carried out 3 years before. This resulted in the Misdemeanour Court issuing the largest penalty fee to date (see 6.1.4 below).

634. Furthermore, the CNB advised that it follows, and monitors deadlines and adequacy of all measures implemented by REs. Whilst the verification of remedial actions will be primarily assessed off–site as and when actions are addressed. Given that the off–site approach is comparable with the on–site approach, the AT is sufficiently satisfied with the effectiveness of this mechanism.

*Financial Inspectorate*

635. The Financial Inspectorate has a reasonable AML/CFT supervisory framework that takes into account the REs' risks. Although, resource limitations prevent the full application of the framework.

[181] In 2016–2017 the Financial Inspectorate was the designated supervisory authority for the Payment Institutions. No on–site or off–site supervision was conducted because the REs did not start trading until 2017, and they were not significant enough to warrant active supervision. The supervision of the sector was transferred to the CNB in 2018.

636. The Financial Inspectorate is composed of highly professional and dedicated staff. However, none of the departments is fully staffed, having from 25% to 85% of vacant positions, including in the unit of higher risk sector – MVTS supervision. Considering that the Financial Inspectorate also covers sectors with thousands of representatives, this could impact its level and effectiveness of supervision. Nonetheless, the AT positively notes that the Financial Inspectorate strives to make the best use of its human resources bearing in mind the risk level of various supervised sectors when deploying its staff.

637. The Financial Inspectorate is required to implement an annual supervisory plan, setting out the supervisory priorities, on–sites, etc. It has documented procedures that set out the sources of information utilised to determine the supervisory plan. This includes: (i) data from the annual questionnaire submitted by REs (the analysis of the questionnaires identified REs who have fundamental deficiencies in its compliance); (ii)risk assessments of RE made by the team, e.g., follow up on–sites, and (iii) desirable supervision cycle, according to REs risk scores.

638. The supervisory cycles are primarily determined by the level of the ML/TF risk of the sector based on the Financial Inspectorates assessment, and then on the individual RE risk score within each sector. The frequency of routine on–site inspections in the DNFBP sector currently ranges: for high–risk sectors[182] (no sector is identified) from 2 years to random selection; for medium–high risk sectors[183] (Accountants, DPMS and TCSPs) and for medium–low risk sectors[184] (Lawyers, Notaries, Real Estate Brokers) from 3 years to random selection; and for low risk sectors[185] (Auditors) from 4 years to random selection. In addition to supervisory cycles, the REs are also requested to fill in questionnaires, the frequency[186] ranging from annual to every five years submission for high risk sectors, to biennium to random selection for the low risk sector.

639. The Financial Inspectorate applies a combination of supervisory tools to FI's, i.e., the MVTS and the Authorised Exchange offices. In the higher ML/TF risk scenarios, they would opt for on–site supervision, and in lower risk scenarios –off–site or collation of data. In addition to these, with these two FIs the Financial Inspectorate also conducts meetings and requests periodic submission of questionnaires.

**Table 6.4: Supervisory engagement for MVTS and Authorised Exchange Offices**

| | High | Medium/High | Medium/Low | Low |
|---|---|---|---|---|
| Nature of the supervision | On–site<br>Off–site | On–site<br>Off–site | On–site<br>Off–site | Off–site |
| Supervision cycle | 2 years | 4 years | 5 years | Random selection |
| Meetings | Annually | 2–4 years | As needed | As needed |
| Questionnaires | Annually | 2 years | 2 years | 3 years |

640. As can be seen from the above description, the supervisory cycles do appear to be quite lengthy. More so, considering that the Financial Inspectorate does not have any sectors classified

[182] High risk – 2 year, Medium–high risk – 4 years, Medium–low risk – 5 years, Low risk – random selection.
[7] High risk – 3 year, Medium–high risk – 4 years, Medium–low risk – 5 years, Low risk – random selection.
[184] High risk – 3 year, Medium–high risk – 5 years, Medium–low risk – random selection, Low risk – random selection.
[185] High risk – 4 year, Medium–high risk – 6 years, Medium–low risk – random selection, Low risk – random selection.
[186] High risk sector: High risk – annual, Medium–high risk – 2 years, Medium–low risk – 3 years, Low risk – 5 years.
Medium–High risk sector: High risk – annual, Medium–high risk – 2 years, Medium–low risk – 4 years, Low risk – 7 years.
Medium–Low risk sector: High risk – 2 years, Medium–high risk – 3 years, Medium–low risk – 5 years, Low risk – random selection.
Low risk sector: High risk – 2 years, Medium–high risk – 4 years, Medium–low risk – 6 years, Low risk – random selection.

as high risk, its supervised REs are subject to cycles commencing at 3 year intervals. Nonetheless, the off–site supervision and the annual questionnaires supplement the on–site work.

641. The off–site risk assessment reports evidenced this is a comprehensive process and includes a review of the REs internal documentation and client files. Off–site supervision will also result in feedback provided to firms setting out remediation plans, and where necessary, the submission of indictment for any breaches identified. The combination of the off–site supervision with the questionnaires provides comprehensive data for the Financial Inspectorate to periodically assess the ML/TF risks of its REs.

**Table 6.5: Number of on–site supervisions[187]**

| | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | No of REs | No. of on–sites | No of REs | No. of on–sites | No of REs | No. of on–sites | No of REs | No. of on–sites | No of REs | No. of on–sites |
| MVTS | 15 | 1 | 39 | 3 | 55 | 3 | 65 | 1 | 52 | 1 |
| Accountants, auditors & tax advisory services | 5640 | 14 | 5640 | 17 | 5435 | 14 | 5435 | 8 | 5435 | 23 |
| DPMS | 380 | 3 | 380 | 5 | 108 | 4 | 108 | 7 | 108 | 5 |
| TCSPs | 2 | 0 | 1 | 1 | 1 | 0 | 1 | 2 | 1 | 0 |
| Exchange offices | 1309 | 123 | 1291 | 140 | 1296 | 81 | 1228 | 81 | 1188 | 40 |
| Lawyers | 3483 | 12 | 3545 | 10 | 3569 | 6 | 3669 | 6 | 3669 | 8 |
| Real estate brokers | 886 | 8 | 1025 | 0 | 1008 | 16 | 912 | 4 | 1198 | 7 |
| Notaries | 312 | 5 | 327 | 6 | 330 | 2 | 327 | 3 | 327 | 4 |

642. The table above demonstrates that the Financial Inspectorate focuses its resources on sectors posing a higher risk, as during 2016–2020 it carried out on–sites on 17% of the MVTS sector, 39% of the Authorised Exchange Offices. Thus, the number of on–sites appear to be aligned to the Financial Inspectorate methodology. The Financial Inspectorate is commended for maintaining this level of supervision considering it is significantly under–resourced. As noted above, figures show that the Financial Inspectorate overall is resourced only at approx. 50% of its capacity (with some departments having less than 25% of staffing).

643. The Financial Inspectorate shortage of resources and available IT support, has resulted in a shift in the type of supervision with a reduction of on–site inspections and increase of off–site supervision. Nonetheless this has not affected the overall quality and effectiveness of the supervisory regime.

*CFSSA*

644. The CFSSA's AML/CFT supervisory framework is not sufficiently detailed to consider it effective, and given the limitations in risk understanding noted in the section above, the supervisory framework does not adequately take into account the RE's risks. Furthermore, the overall level of supervision is also considered insufficient.

645. The CFSSA has one team with responsibility for the AML/CFT supervision of all its sectors. The AML/CFT Supervision team is comprised of 2 individuals, with 1 vacant position. They hold responsibility for approx. 75 REs.

[187] The order of the sectors follows the risk rating of the sector given by the Financial Inspectorate sectoral risk analysis

646. The CFSSA is required to implement an annual supervisory plan, setting out the supervisory priorities, on–sites, etc. Copies of the last few years were provided, however, the focus on this plan is prudential related risks, e.g., solvency in respect to life insurance companies.

647. The CFSSA's Rules of Procedures also determines the supervisory cycle depending on the type of entity and risk score. This includes on–site and off–site supervision. However, this does not seem to be followed, in practice, as there is no formal calendar for future inspections or follow–ups, and authorities were unable to explain what factors are used to determine why a firm is selected to be inspected as part of the established annual supervisory plan.

**Table 6.6: CFSSA – Number of on–site supervisions**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No. REs | No. of on–sites | No. REs | No. of on–sites | No. REs | No. of on–sites | No. REs | No. of on–sites | No. REs | No. of on–sites | No. REs | No. of on–sites |
| Life Insurance companies | 14 | 3 | 13 | 0 | 13 | 3 | 12 | 0 | 11 | 0 | 11 | 1 |
| Subsidiaries of foreign life insurance companies | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 |
| Investment funds management companies | 21 | 9 | 21 | 3 | 21 | 3 | 20 | 0 | 23 | 1 | 20 | 1 |
| Pension companies managing voluntary pension funds | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 4 | 1 |
| Pension insurance companies | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 2 | 0 |
| Pension funds management companies | 6 | 0 | 6 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Investment firms | 8 | 3 | 8 | 0 | 7 | 0 | 7 | 0 | 7 | 0 | 6 | 1 |
| Factoring companies | 13 | 0 | 13 | 0 | 9 | 0 | 7 | 1 | 6 | 2 | 4 | 0 |
| Leasing companies | 21 | 2 | 19 | 0 | 17 | 0 | 16 | 0 | 14 | 0 | 15 | 0 |
| VASPs | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | 15 | 0 |

648. Off–site supervision is said to consist of questionnaires that request quantitative and qualitative data. Furthermore, off–site supervision also collates data held by the authorities, such as complaints, and data held by other supervisory bodies such as the European Supervisory Authorities (ESA). The frequency of submission of questionnaires by REs is dependent on the sector and the risk profile of the RE, ranging from annually for high–risk leasing companies and VASPs to as necessary for lower risk REs, and every two years for all other sectors regardless of their risk profile. Furthermore, the CFSSA has not demonstrated the receipt of this information, nor to what extent an assessment is carried out on this data, nor if this analysis drives or impacts the supervision of the CFSSA.

649. The level of supervision carried out by the CFSSA is not sufficient. As can be seen from the table above, the percentage of REs subject to an on–site was between 2015: 19%, 2016:3.6%, 2017:7.9%, 2018:1.4%, 2019:4.4% and 2020:5.1%. Prior to 2020, the on–sites noted in the table above were not specific to AML/CFT, hence, the extent of the AML/CFT review during these on–sites is unknown.

650. The CFSSA also indicated that any new circumstances might trigger an overall risk assessment, including on–site inspection, e.g., changes in business plan such as new risk clients or services, information on the BOs, the implementation of remedial actions, etc. Given the low number of on–site visits, it appears that either the triggers have not been identified by the CFSSA team or the threshold to carry out an on–site is significantly high.

*Tax Administration*

651. The TA does not allocate any dedicated resources to the AML/CFT supervision of the casinos. The staff responsible for tax audits are also required to carry out AML/CFT supervision.

652. The TA does not have a specific AML/CFT supervisory regime. It does establish annual supervisory plans however, these are primarily driven by the need to conduct a tax audit and then AML/CFT if factored in. Furthermore, the TA was unable to evidence how firms were selected for an on–site, e.g., what factors would trigger an on–site inspection.

653. The TA has provided no information or supporting documents on the risk scoring of the casinos, therefore, the evaluation team considers that these REs do not have a risk score assigned that would determine the level of supervision based on the risks posed by each.

654. The TA has not provided any internal policies or procedures to evidence its supervisory approach or a risk–based approach to supervision. Therefore, it was unable to demonstrate if its supervision is effective in identifying, managing, and mitigating ML/TF risks.

**Table 6.7: TA – Number of on–site supervisions**

| | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **No. REs** | **No. of on–sites** | **No. REs** | **No. of on–sites** | **No. REs** | **No. of on–sites** | **No. REs** | **No. of on–sites** | **No. REs** | **No. of on–sites** |
| Casinos | 15 | 3 | 15 | 4 | 19 | 4 | 19 | 3 | 22 | 1 |

### *6.2.4. Remedial actions and effective, proportionate, and dissuasive sanctions*

655. Supervisory authorities demonstrated taking remedial measures, but the effectiveness and number of these vary across the supervisors being stronger at the CNB and weaker at the TA. The most frequently applied types of sanctions are written warnings and fines, which are not deemed effective enough. Other types of sanctions are rarely or never applied, e.g., removing individuals from holding a key function, which is a matter of concern.

656. All supervisory authorities have the legal powers to impose sanctions directly on REs under Art.233 and Art.228 of the Misdemeanour Act. Whilst under the AMLTFL, the Council for Misdemeanour Proceedings (within the structure of the Financial Inspectorate) is authorised to impose monetary sanctions, and the supervisory authorities are limited to supervisory sanctions such as written warnings, issuing a formal decision to request REs to address violations or the withdrawal of an authorisation. All supervisory authorities advised that their preferred option when considering a monetary sanction is to submit an indictment to the Council for Misdemeanour Proceedings to process and make the final decision. The reason for this is

primarily the cost and resources required to process the sanctions and subsequent appeals process that is common from REs. It appears that REs are more reluctant to appeal a decision by the Council for Misdemeanour Proceedings than from a supervisory authority. Only rarely the decision of the Council for Misdemeanour Proceedings is challenged to High Misdemeanour Court.

657. With respect to investigations referred to the Council for Misdemeanour Proceedings, supervisory authorities may commence the process of reaching a regulatory settlement agreement with a RE instead of issuing an indictment. However, the details and conditions of the settlement agreement need to be referred to and agreed upon by the Council for Misdemeanour Proceedings. This approach is utilised by the CNB and Financial Inspectorate. Neither the CFSSA nor the TA provided any information in this respect.

658. The CNB has some written policies, however, these are not detailed enough to determine the CNB's approach to sanctions. Nonetheless, the CNB confirmed that it would submit an indictment to the Council for Misdemeanour Proceedings for all breaches identified, regardless of nature or seriousness. The Financial Inspectorate has documentation setting out how it makes use of these supervisory powers. The policy sets out various levels, factors and thresholds that determine what actions the Financial Inspectorate will take. It will submit an indictment to the Council for Misdemeanour Proceedings when breaches are considered of a serious nature.

659. The Council for Misdemeanour Proceedings of the Financial Inspectorate is responsible for all misdemeanour proceedings in the first instance by applying the Misdemeanour Act. The Council consist of three law graduates, of whom the president of the Council must have passed the bar exam. When determining monetary sanctions, the Council is required to consider the degree of guilt, the danger of the offence and the purpose of the punishment. The Council should also take into account mitigating and aggravating circumstances, e.g., financial position, motives, historical conduct, and other personal causes that may have contributed to the misdemeanour. After the Council takes a decision, the matter may then be referred to the High Misdemeanour Court, if deemed necessary or if the decision has been appealed. The decision on the misdemeanour proceeding is announced orally at the hearing and is published on the MoF website no later than three days from the day of the end of the hearing. A written copy of the decision with an explanation is formally delivered to all parties.

**Table 6.8: Number and amount of penalty fees imposed on FIs**

| | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) |
| Banks (including House Savings Banks and Credit Unions) | 2 | 9 867 | 11 | 40 987 | 6 | 48 567 | 1 | 11 467 | 11 | 4 479 999 |
| E–Money Institutions | 0 | 0 | 5 | 7 587 | 0 | 0 | 0 | 0 | 0 | 0 |
| MVTS | 0 | 0 | 0 | 0 | 1 | 45 333 | 1 | 25 667 | 1 | 13 400 |
| Exchange offices | 2 | 24135 | 2 | 61683 | 2 | 4 444 | 8 | 16 728 | 11 | 21 720 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Life insurance companies | 2 | 21 333 | 2 | 48 639 | 0 | 0 | 0 | 0 | 0 | 0 |
| Investment funds management companies | 4 | 0 | 3 | 3 773 | 0 | 0 | 0 | 0 | 0 | 0 |

660. No financial sanctions were applied on consumer credit, leasing, factoring, pension insurance companies. Over the same period of time, in addition to fines, there were 122 written warnings issued by the supervisory authorities, most of which were addressed to the Exchange offices (86) and Banks (18), followed by the Payment Institutions (9), Investment Funds (4), Life Insurance (2), and Factoring (2).

**Table 6.9: Number and amount of penalty fees imposed on DNFBPs**

| | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) | No. of Res sanctioned | Total Penalty fees (EUR) |
| Lawyers | 3 | 13 342 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Notaries | 1 | 7 986 | 1 | 4 040 | 1 | 2 020 | 1 | 7 714 | 1 | 1 067 |
| Accountants, Auditors and Tax Advisors | 0 | 0 | 3 | 29 697 | 2 | 4 956 | 0 | 0 | 1 | 4 267 |
| Real Estate | 5 | 32 761 | 2 | 23 031 | 0 | 0 | 0 | 0 | 0 | 0 |
| Dealers in Precious metals | 0 | 0 | 1 | 404 | 0 | 0 | 6 | 69 764 | 0 | 0 |

661. No financial sanctions were applied on TCSPs and casinos over the analysed period, but the statistics indicate that there were some inspections conducted on casinos.

662. With the exception of one bank that was fined EUR4 4mln. in 2020, during 2016–2020, the average fine imposed on a bank was EUR6 362, the average for authorised exchange offices being EUR5 148, and on MVTS being EUR28 133.

663. Generally, the sanctions imposed on REs are not considered by the AT as effective and dissuasive. As can be seen from the table below, very few penalties have been imposed, and the amount of these are relatively insignificant in some cases, considering the turnover of some REs. Particularly in respect of the Banks, during 2016–2020, the sanctions are considered too low to have any significant impact. Although the CNB notes that lower monetary sanctions have been supplemented with remedial actions, this is considered further in Section 3.2.5 below.

664. The fines imposed on exchange offices are more aligned because these types of businesses will have a lower turnover. Of 465 on–sites carried out in the sector, 25 REs have been fined and 86 written warnings. Similarly, monetary sanctions imposed on the MVTS appear to be more aligned with their expected turnover, i.e., fines averaged EUR28 133. In addition, there are a number of sectors that have not been subject to any sanctions partly due to a lack of or limited supervision of these sectors; and other than penalty fines, other types of sanctions are rarely, if at all, used. Lastly, the TA also noted that when there are misdemeanours in respect to various legislative Acts, e.g., AMLTFL and the supervisory acts, the penalty imposed will be the lowest applicable across the various Act. This will weaken the effectiveness and dissuasiveness of

sanctions. Nonetheless, the AT positively notes Croatia's efforts to apply more stringent monetary sanctions as from 2020 given the greater powers implemented in 2019.

**Table 6.10: Fines imposed on individuals (for all supervisory authorities)**

| Year | No. of Individuals | Total Amount (EUR) |
|---|---|---|
| 2016 | 31 | 25 898 |
| 2017 | 20 | 16 707 |
| 2018 | 33 | 17 353 |
| 2019 | 17 | 10 693 |
| 2020 | 22 | 29 960 |
| **TOTAL** | **123** | **100 611** |

665. As can be seen from the table, the average fine on an individual is EUR 817. While it is understood that across the sectors, the materiality varies, and there is a considerable range between the minimal and maximal size of applied monetary sanctions, overall, these are not considered as dissuasive, particularly in respect of sectors such as banks. The supervisory authorities noted that when they submit an indictment, the investigation will consider breaches by the RE and any individuals holding responsibility for AML/CFT. The AT positively observes the common practice for the final decisions to impose monetary sanctions on the RE and on individuals holding key functions.

666. The power to remove individuals from holding a key function has never been used. Given that the CNB and the Financial Inspectorate seem to have a greater number of cases where an individual and/or a RE has been imposed a fine, the AT questioned the reasons for not taking regulatory action in respect to the removal or suspension of key individuals. The Financial Inspectorate considered that sometimes it is a quicker and easier process to allow the individuals or the RE to voluntarily cease its function or trading. The CNB also noted that if individuals resign, the only sanction possible is a monetary fine. For example, in the case noted below in respect to a Bank, no action has yet been taken against the management and supervisory bodies of the Bank. However, all members of the management and supervisory bodies have resigned from their positions upon the own decision of the company. This is an area of concern because individuals may re–apply for key functions within other REs in Croatia or other jurisdictions, and there may be no documented adverse information against them that would impact their fitness and properness.

667. Another concern noted by the AT is the timeliness of the sanctions process. For example, in the case noted below, the CNB advised that it first initiated proceedings against the bank and then proceedings against seven individuals that include the management board and lower–level managers. Whilst a decision has been made within respect to the bank, no decision has yet been made on the individuals. The findings were identified in March 2019, however, 2 years after the on–site inspection, no decision has yet been made to initiate proceedings against the authorised persons.

**Box N°6.6: Sanctions imposed on a Bank**

An AML/CFT on–site was carried out in a bank in March 2019. The on–site covered the following AML/CFT areas: the risk assessment of individual business relationships, conducting due diligence measures, detecting and monitoring suspicious, complex and unusual transactions and reporting suspicious transactions to the AMLO.

The on–site identified a total of thirty–two violations of the AMLTFL. The bank was issued a decision imposing measures to remediate the identified deficiencies and irregularities. The bank

immediately implemented a remediation plan even before the CNB's decision was issued. Among the most important of the implemented measures was the strengthening of the AML/CFT department by doubling the number of staff and a review of its internal controls, which resulted in the termination of a number of business relationships and the incorporation of new standards for risk–taking and assessment and customer monitoring.

On 30 March 2020, the CNB issued the Bank with a Decision notice instructing it to implement a comprehensive and detailed set of 75 measures and actions in order to establish and maintain an effective system for management of ML/TF risks.

Furthermore, the CNB referred the matter to the Financial Inspectorate to commence misdemeanour proceedings. On 30 October 2020, the Financial Inspectorate passed a Decision under which the bank was found guilty. As a result, the bank was fined HRK 33 000 000 (EUR4.4mln.).

668. Furthermore, the power to withdraw an authorisation has rarely been utilised. The Financial Inspectorate has provided only one example of removal of an authorisation (see case below). None of the other supervisory authorities have provided any data or information of cases when an authorisation has been withdrawn by the authority. Hence, there is a gap here in mitigating risks of ML/TF.

**Box N°6.7: Removal of Authorisation of an Exchange Office**

During the supervision of an exchange office, the Financial Inspectorate identified that a RE and the responsible persons of the exchange office did not carry out CDD measures, i.e., established the identity of the parties when performing time–related transactions of foreign cash sales that reach a value of more than HRK 200 000 (EUR 27 000).

The violations related to the year 2011 with misdemeanour proceedings commenced in October 2012. An indictment was filed in February 2014 and completion of the misdemeanour proceedings, including the final judgement of the High Misdemeanour Court of the Republic of Croatia, in January 2017. The decision was received by the Financial Inspectorate in October 2017.

Given the outcome of the misdemeanour proceedings, notification was made to the CNB to remove the exchange office's authorisation. This was finalised in February 2018.

669. The above case also brings into question the timeliness of sanctions, given that it took the Financial Inspectorate 3 years to submit an indictment and a further 3 years for a decision to be made.

670. Also note that all indictments are published on the MoF website and on the relevant supervisory authority website.

### *6.2.5. Impact of supervisory actions on compliance*

671. The Supervisory authorities demonstrated the effects of their supervision on AML/CFT compliance to a varying degree. While not always this was demonstrated in terms of statistics, systemic improvements of the sector, the examples provided evidence that the supervisory findings are followed up, and the detected deficiencies are remediated at an individual, institutional level.

672. The CNB, CFSSA and Financial Inspectorate follow up on remedial actions imposed on REs after an off–site review or on–site visit. The supervisory authorities have noted they rarely identify recurring breaches, though other breaches may still be common. However, there is limited analysis to evidence this.

673. The CNB provided data on the number of remediation actions imposed from 2015 to 2019. This showed 45 in 2015, 36 in 2016, 61 in 2017, 30 in 2018 and 109 in 2019. With the exception of 2019, the 2015–2018 data shows a relatively similar pattern of numbers in remedial actions. The drop in number of remedial actions between 2017 and 2018 could be attributed to the impact of supervision, however, there is no analysis or other information to determine this. The significant increase between 2018 and 2019 could be as a result of the increased focus on the CNB's supervision since 2019. However, similarly, there is no analysis of other information to determine this. With respect to desk–based supervision, the CNB provided an analysis carried out from the annual reviews that evidences that 33% of credit institutions demonstrated an upgrade in their controls.

674. Follow up supervision is carried out solely as off–site reviews. As has been positively noted in section 3.2.3 above, off–site reviews are largely equivalent to on–site supervision, and hence adequate measures are implemented to verify remedial actions.

**Box n°6.8: Improvement of compliance with AML/CFT requirements following an on–site examination of CNB**

An AML/CFT on–site inspection of a bank was carried out by the CNB in May 2015. The on–site covered nine key areas of the AML/CFT system, establishing weaknesses and deficiencies in six of them and issuing ten recommendations for improvement. The most significant weaknesses were established in the organisational structure and lack of personnel resources, the AML/CFT system application support, due diligence and education. As regards the area of CDD, it was established that the bank had failed to conduct all EDD measures, with the result that the report recorded a misdemeanour for which a fine was imposed to the bank under the misdemeanour proceedings.

The following AML/CFT on–site inspection of the bank was carried out in June 2018. There were no established violations of legal provisions and weaknesses were established only in two examined areas. The bank implemented all recommendations from the previous inspection. The bank considerably improved all elements of its AML/CFT systems, most of all the organisational structure and resources. A new authorised person and authorised person's deputy were employed full time, and the bank's management board was extended by appointing a member in charge of AML/CFT. The investment into personnel contributed the most to the improvement of the overall AML/CFT system through an increase in awareness and corporate culture improvement, stepped up investment into IT support and better education of employees.

675. Similarly to the CNB, follow up supervision is carried out solely as off–site reviews that are largely equivalent to on–site supervision, hence adequate measures are implemented to verify the remedial actions. The Financial Inspectorate reported 2 cases where formal directions were issued to the REs as they had not implemented the remedial actions within the pre–determined deadline. With respect to the MVTS sector, the supervisor advised that it had seen a reduction in remedial actions and a decrease in the overall risk scores of the sector. Improvements were observed by the Financial Inspectorate in the performance of the DNFBP sector.

676. The CFSSA provided some case examples where the supervised entities had improved the internal procedures and reorganised its business activities as a result of a supervisory inspection. While the CFSSA does not conduct supervision of the VASP sector for implementation of AML/CFT measures, steps taken by the CFSSA to engage with the VASPs for registration purposes had a positive secondary impact on the sector, as discussions with the major market players increased that attention towards implementation of the AML/CFT measures increases.

677. The TA has also provided individual examples of the impact of its supervisory actions. In particular, as a result of detected deficiencies, the inspected REs improved their internal procedures, including related to assessment of their ML/TF risks and implementation of the CDD measures, and also reorganised their operations to improve compliance with the legislative requirements.

678. Though the evaluation team note the positive impact of the supervisory action on enhancing compliance with the AML/CFT requirements, the overall low number of on–site inspections for some sectors, and low number of sanctions issued for sectors with a higher materiality such as Banks, remain a concern.

### *6.2.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks*

679. The supervisory authorities support the REs in raising understanding of their AML/CFT obligations in various ways, including by providing guidance, trainings, and some, also through conducting supervisory dialogues.

680. The AMLTFL requires the supervisory authorities to issue guidelines on various matters, including on conducting ML/TF risk assessment by the REs, related to conducting CDD, applying enhanced and simplified measures, identification of a customer and verification of his identity when done remotely, non–face–to–face, etc. All supervisory authorities have implemented these measures as also described under R.34. All the guidelines are also published on the respective supervisor's websites. All sectors were aware of the guidance and other information issued by supervisory authorities and are required to comply with them.

681. Another example is the provision of harmonised guidelines recently issued in respect to the use of electronic verification of customers' identification. This approach was adopted by all three supervisory authorities (CNB, Financial Inspectorate and CFSSA), and across all sectors under their supervisory remit. Furthermore, any feedback provided to REs on legislative interpretation is referred to and agreed with AMLO, to ensure consistency in approach.

682. The CNB, the CFSSA and the Financial Inspectorate have evidenced a significant amount of engagement with their sectors, covering AML/CFT obligations and ML/TF risks, offering annual training, and providing support to RE on individual queries.

683. The CNB conducted outreach on various topics, with a focus on ML/TF risk assessment, application of preventative measures, use of new technologies, etc. CFSSA holds meetings with REs in relation to implementation of the AML/CFT requirements, as well as other matters when necessary. Outreach is also conducted upon REs' request, where additional explanations and guidance are required. The Financial Inspectorate organised periodic meetings with the supervised FIs with a special focus on the MVTS sector, which is considered to have a higher ML/TF risk, and significant volume of turnover. Trainings were offered to accountants, auditors and real estate brokers. Financial Inspectorate holds thematic meetings with representatives of chambers and other DNFBP associations on implementation of the provisions of the AMLTFL. The

TA itself is not active in reaching out to the gambling sector but indicated that the Croatian Gambling Operators Association conducts annual trainings for the representatives of the sector on application of the AMLTFL.

**Table 6.11: Training and other engagement per authority**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| **CNB** | 2 | 1 | 4 | 4 | 3 |
| **CFSSA** | 3 | 3 | 2 | 2 | 2 |
| **FI** | 6 | 2 | 7 | 4 | 3 |

684. The AMLO co–operates intensively with the supervisory authorities on all matters of training, guidance, etc., coordinating the action in order to better focus the efforts. The AMLO assists the supervisory authorities on training sessions, and review and agree on guidance documents, and assists in providing individual assistance to REs. Similarly, supervisory authorities attend training sessions provided by AMLO to the private sector – Annual Conferences. In fact, the AMLO has been the largest contributor to training the private sector, providing 11 training sessions in 2018, 9 in 2019, and 6 in 2020. The training offered ranged from a generic understanding of AML/CFT obligations to NRA related matters, typologies, etc. The examples of the training materials were of good quality.

**Box N° 6.8: Raising awareness of REs providing MVTS**

The Financial Inspectorate identified common issues and breaches in the MVTS sector, therefore, it agreed with AMLO to provide sector–specific training to address these concerns.

A specialist workshop was delivered in October 2018 where REs were taken through the legal requirements and the application of such, specifically to the MVTS sector.

The workshop focused on; reporting STRs, risk assessment obligations, CDD requirements in respect to occasional transactions, and ongoing monitoring. The training also took the opportunity to cover the results of the NRA and the contents of the SNRA, specifically focusing on the sector's assessment.

*Overall conclusions on IO.3*

685. The AT has afforded a higher weighting to the supervisory measures implemented for the most important and important sectors, i.e., Banks, MVTS, Authorised Exchange Offices, Casinos and VASPs.

686. The level of AML/CFT licensing, risk understanding in the supervised sectors and risk–based supervision varies across the supervisory authorities, but overall is demonstrated to be considerably stronger at the CNB and the Financial Inspectorate. These two are responsible for the most important and majority of important sectors. Performance in terms of implementation of AML/CFT supervisory measures are weaker at CFSSA and to a larger extent at the TA, which are responsible for less material sectors.

687. All FIs and DNFBPs are covered by licensing and registration requirements, except for newly regulated VASP sector, where notification mechanism is introduced and some less material DNFBPs (accountants, TCSPs and DPMS). While in financial sector there are mainly adequate measures implemented, concerns remain with measures to prevent criminal associates from holding key functions within the DNFBP sectors. While framework for effective approbation of sanctions is in place, sanctions particularly for higher risk sectors, such as Banks were not

effective or dissuasive. The utilisation of wider scope of other sanctions such as the removal of individuals from key functions when adequate, is an area for further improvement.

688. Taking into consideration the performance of the licensing and supervisory authorities responsible for the most material and the majority of material sectors, the deficiencies in place entail that in order to ensure effective performance across the competent authorities, only major improvements are required.

689. **Croatia is rated as having a Moderate level of effectiveness for IO.3**.

# 7. LEGAL PERSONS AND ARRANGEMENTS

## 7.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 5***

a) Information on the creation and types of legal persons and arrangements is publicly accessible. This includes the legislation and additional guidelines and, explanatory notes. There is, however, not sufficient publicly available information highlighting the requirement to register with the BO Register for foreign trusts from non–EU Member States and when establishing a legal person in Croatia.

b) The authorities independently of each other demonstrated some understanding of vulnerabilities of legal persons, which were based on observations of their operational practices. However, a large amount of information in possession of authorities was not consolidated and analysed in a systemic manner to assess the vulnerabilities of various types of legal persons the extent to which legal persons created or registered in Croatia can or are being misused for ML/TF. No analysis and limited understanding were displayed with respect to legal arrangements (confined to foreign trusts) operating in Croatia. TF vulnerabilities of legal persons and arrangements are not explored. While observing that the LLCs and Simple LLCs are the types of legal persons that are most frequently abused, Croatian authorities are reluctant to flag certain types of legal persons as the most vulnerable vehicle for ML, rather are inclined to focus on the schemes and criminal conduct itself.

c) Croatia has in place a range of measures to mitigate the misuse of legal persons and arrangements, such as the requirement to register in various registers (Court Register, Register of Foundations, Register of Foreign Foundations, Register of Associations, Registered of Foreign Associations), and recently, with a BO Register which has been operational since January 2020. All of these registration mechanisms, nevertheless, have weaknesses related to prevention from misuse of legal persons and arrangements by criminals due to: deficiencies in the types of information gathered; overreliance on self–declarations; poor verification; and lack of ongoing monitoring of changes. In addition, authorities involved in the registration process displayed mutual reliance on the quality of each other's performance, thus not enforcing checks and controls that form the basis of this registration mechanism. Exchange of information between the Registers and the BO Register needs to be developed.

d) Timely access to information is sought to be provided through various registers operating in Croatia that make the basic information publicly accessible to any interested party. Access to the BO Register is granted to all Croatian authorities. Copies of documents kept with the registers are also easily accessible in a timely manner. Adequacy of information casts doubts in some instances. Issues with verification of information and ongoing monitoring undermine the accuracy of

the information and how up to date it is. This is to some extent mitigated by the availability of alternative sources of information, including REs and legal persons and arrangements themselves.

e) Croatia did not provide appropriate data to comprehensively demonstrate the extent to which application of sanctions is effective. Nevertheless, it appears that there were cases of application of penalty charge notices for late notification of information and rejection of registrations, such as for omitting supporting evidence and the application not being in accordance with the law. The monetary penalties in place may be effective if applied. No sanctions are applied for failure to provide information to the BO Register because of the application of a moratorium triggered by the COVID–19 and applied with an undefined deadline.

***Recommended Actions***

***Immediate Outcome 5***

a) Croatia should: (i) conduct an in–depth risk assessment of legal persons and arrangements created and operating in Croatia to identify, assess and understand their vulnerabilities and potential for ML/TF abuse (ii) communicate the outcomes to competent authorities and the private sector; and (iii) take adequate measures to mitigate the identified risks.

b) Mechanisms should be introduced by Croatia to ensure: (i) verification of all information provided at the stage of registration of a legal person; (ii) prevention of criminals (ML, predicate offences and TF) from acting as a shareholder, BO, or manager of a legal person, introducing a requirement for verification of criminal background of these persons, including implementation of the UN TFS measures; (iii) introduction of an ongoing monitoring mechanism for ensuring timely detection and registration of changes to basic and BO information, (iv) implementation of a mechanism for supervision to ensure the accuracy and timely update of information; and (v) imposition of effective, proportionate and dissuasive sanctions for failure to comply with the information requirements, and compiling and maintain statistics on application of sanctions. This should be followed by assignment of clear responsibilities for authorities with supervisory function, allocation of adequate resources, and regular supervision.

c) Croatia should define the criteria for the change in situation which would terminate the moratorium on application of sanctions for filing information in the BO Register and conduct analysis of comprehensiveness of the BO database – adequacy, accuracy and timeliness of the submitted information.

d) Croatia should develop a mechanism of co–operation and coordination between the Registers of legal persons and arrangements (Court Register, Register of Foundations, Register of Foreign Foundations, Register of Associations, Registered of Foreign Associations), and the BO Register, to ensure consistency of information and timely notification about pertinent changes.

690. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R R.24–25, and elements of R.1, 10, 37 and 40.[188]

691. The assessment team based its conclusions on a variety of information provided by the authorities, including discussions held with relevant REs during the on–site, and qualitative and quantitative information maintained by Croatia, including findings of the NRA, STRs and criminal cases. Open–source information was also used to support the findings of the AT.

## 7.2. Immediate Outcome 5 (Legal Persons and arrangements)

### *7.2.1. Public availability of information on the creation and types of legal persons and arrangements*

692. The laws regarding the creation and types of legal persons in Croatia are publicly available online: www.zakon.hr.

*Companies*

693. Requirements to set up companies and institutions in Croatia are set out in the Companies Law, the Institutions Law, and the Court Register Law. A public website provides a list of all types of companies available in Croatia by following links on: Companies – Point of Single Contact (psc.hr). Details on companies based on capital are only available in Croatian. Publicly available data on the government websites provides simplified information on how to set up a business and provides further links to how to set up: (i) a JSC or an LLC via a notary[189], and (ii) an LLC and SLLC online[190] (accompanied with information about SLLCs[191]). There is no information other than the statutes on how to set up an institution.

694. There is a concept of a secret society in Croatia. The Secret society, which is not a legal person, but a contractual arrangement for one party (the secret member) to obtain the economic benefit of another person's business (the entrepreneur). This arrangement is regulated under the Companies Law, which is a publicly available document.

*Association and Foundations*

695. Requirements to set up associations and foundations are contained in the Foundations Law and the Associations Law. Registration is also required for foreign foundations and associations operating in Croatia, which are governed by the same legal acts. The MoJA website provides comprehensive information and guidance on registration of domestic and foreign foundations and associations[192]. In addition, the e–citizen portal has detailed guidance on establishment and registration of associations[193]. Information[194] and a form to set up an association is available

[188] The availability of accurate and up–to–date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.
[189] Founding a society – gov.hr
[190] User Instruction (gov.hr)
[191] Founding j.d.o.o. – gov.hr
[192] Ministry of Justice and Administration of the Republic of Croatia – Insight into registers (gov.hr)
[193] https://gov.hr/hr/osnivanje–i–registracija–udruga/568
[194] https://mpu.gov.hr/registar–udruga/22213

online[195] with a list of documentary requirements, which are submitted to the administrative body of a county or the City of Zagreb (local–self administration bodies) directly or by post.

*Trusts*

696. Croatia does not have a Trust Law and is not a signatory of the Hague Convention on the Law Applicable to Trusts and on their recognition. In line with the AMLTFL, unless a foreign trust can provide evidence of legal recognition in an EU Member State, they are required to register in the BO Register if they form a business relationship with a RE or purchase real estate. The webpage of FINA[196] contains information on the requirement for registering the trust. No other public government source (in particular the land registry website) provides guidance or reference to a need for the trust to register with the BO Registry.

697. By 31 December 2019, legal persons must have registered with the BO Register retained by the Finance Agency on behalf of the AMLO. Nevertheless, the online guidance on establishment of legal persons does not make a reference or provides for links to the explicit requirement for registering in the BO Register. There is standalone guidance on requirements to register with the BO Register publicly available on a number of websites, namely, such as e–citizen, MoF and FINA197. Authorities described that when the BO Register was introduced, they had undertaken an extensive outreach program via web pages, online trainings, notices to professional service providers, notices to state administration offices, notices directly via the TA to all legal persons. The AMLO responded to over 5 000 written and telephone enquiries relating to the BO Register from 3rd June to 31 December 2019 (7 months).

### *7.2.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities*

698. No comprehensive assessment of vulnerabilities of the different types of legal persons and arrangements, and what characteristics and features make them vulnerable to ML/TF in Croatia is included in either the 2016 or the 2020 NRA. Legal persons are often misused for ML, especially through tax evasion and fraud. The use of frontmen to conceal the real ownership**,** setting up complex corporate structures involving foreign entities, use of fictitious companies have been detected, in practice as ways to launder and conceal the proceeds of crime**.** Croatia possesses information on trends and typologies, including criminal cases, which highlighted that the LLCs and Simple LLCs are the types of legal persons that are most frequently abused. Croatian authorities are reluctant to flag certain types of legal persons (LLCs and/or Simple LLCs, which are the most prevalent) as the most vulnerable vehicle for ML, rather, they are inclined to focus on the schemes and criminal conduct itself.

699. TF vulnerabilities of legal persons and arrangements are not explored. Nevertheless, conclusions about the overall low TF risk in Croatia give authorities comfort that the vulnerabilities of the legal persons for TF are also low. Authorities consider that this is also confirmed by the practical examples. While over the past period there were STRs filed by REs with suspicion of TF and legal persons were involved, the pre–investigative actions conducted

[195] Ministarstvo pravosuđa i uprave Republike Hrvatske – Elektronički upis u registar (gov.hr)
[196] https://www.fina.hr/registar–stvarnih–vlasnika
[197] E citizen: Register of beneficial owners – gov.hr and on Ministry of Finance of the Republic of Croatia – Register of Beneficial Owners (gov.hr) and FINA: Register of beneficial owners – Fina

did not lead to any investigations and prosecutions of legal persons for TF in Croatia to confirm the actual misuse of legal persons for TF. An example of such a report is provided below:

**Box N°7.1: TF STR related with Simple LLC**

In March 2018 the AMLO received an STR from a bank in relation to a Croatian company – a Simple LLC. The bank refused to carry out a transaction in the amount of EUR 4 315, which was to be executed in favour of the Croatian Simple LLC account by a foreign company, which was suspected to be on the sanctions list due to suspicion of TF.

The AMLO conducted analysis and disseminated the case to the SIA. The latter conducted a comprehensive operational analysis found no link to TF and informed the AMLO. LEAs were not involved.

700. The AMLO published trends and typologies of ML in its annual reports and issued a book of consolidated ML typologies, where, in a number of schemes, legal persons were used for committing ML. The AMLO detected cases of abuse of national and foreign legal persons. While the initial focus of the AMLO was on detecting the schemes in which legal persons were abused, it had also formed a knowledge about the types that are affected most frequently, their ownership structures and geography. Respectively, these appeared to be LLCs and Simple LLCs whether set up in Croatia or in a foreign jurisdiction (often neighbouring jurisdictions or an off–shore zone).

701. AMLO's analysis of common schemes for ML abusing legal entities among others include the following ones: (i) receipt of non–cash incoming transfers for the same economic activity followed by immediate withdrawal of funds; (ii) absence of substance to the company with no payments to staff or business premises, or apparent income generating activity with money paid in and out without rational explanation; (iii) structuring of payments in a number of transactions to avoid thresholds; (iv) use of fictitious invoices for sales of goods; (v) setting up banks accounts in Croatia by foreigners through "money mules"; (vi) use of strawmen to set up companies (such as people who are homeless, have special needs or have dual Croatian nationality and leave the jurisdiction).

702. According to information provided by the MoI, while not specifying the types, between 2015–2020, there were six legal persons reported for the criminal offence of ML. In these cases, the predicate offences were: (i) abuse of trust in economic transactions (CC, Art.246), (ii) forgery of official or business documents (CC, Art.279), (iii) fraud in economic operations (CC, Art. 247), and (iv) computer fraud (CC, Art.271).

703. The Serious Organised Crime Threat Assessment for 2019 to 2020 conducted by the MoI contains analysis of the methods for abuse of legal persons, using them as a "façade of legality". These detected patterns include: setting up or acquiring legal persons by members of OCG in Croatia and other EU Member States; establishing control over legitimate private companies applying pressure on the senior management; infiltration of members of OCG into high positions within business entities in order to control their work.

704. In addition, the SAO conducts an annual analysis of criminal complaints filed against legal persons, indictments achieved, and convictions granted. These analysis does not identify the type of legal persons but provides a general review of the offences where legal persons were involved indicated three of the most frequent to be breach of trust in business operations; fraud in business operations; and tax and customs evasion.

**Table 7.1: SAO Annual reports 2015–2020 on investigation, prosecution a conviction of legal persons**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| Criminal complaints filed (Number of legal persons) | 1 331 | 1 431 | 1 263 | 1 188 | 1 055 | 1 345 |
| Investigations conducted (Number of legal persons) | 97 | 135 | 85 | 95 | 101 | 108 |
| Indictments after investigation/direct (Number of legal persons) | 97/159 | 65/142 | 86/53 | 50/111 | 43/53 | 132[198] |
| Convictions (Number of legal persons) | 95 | 104 | 68 | 28 | 71 | 75 |
| Confiscated assets (EUR) | 706 872 | 1 799 629 | 397 290 | 74 300 | 107 641 | 14 466 |

705. So far, Croatia has not detected criminal offences committed with the use or involvement of trusts or any type of a legal arrangement, that is recognised and regulated in Croatia. Considering the complex nature of these structures, it is challenging to detect criminal schemes conducted through these vehicles and understand the related ML/TF risks.

706. The NRA contains a limited assessment of transparency of legal persons and arrangements in Croatia. It outlines identification of BOs and directors/management of legal persons upon establishment, which promotes transparency and reduces the risk of misuse of legal persons. The NRA does not contain a systematic analysis of the characteristics of legal persons and the features of the Croatian system that make them vulnerable, e.g., lack of checks at the stage of registration; online registration of companies; very low requirements for share capital (for LLCs and Simple LLCs); lack of supervision, monitoring, and sanctions for submission of inaccurate information; use of shelf companies; use of a frontman; setting up secret societies; operation of foreign–registered companies in Croatia; setting up of companies in Croatia by foreign nationals or legal persons, etc.

707. There is also no analysis of the impact of the legislative framework on the law enforcement efforts, i.e., the SAO annual reports indicate that there are extensive barriers to obtaining convictions against legal persons such as: criminal offences which in their legal description do not contain as an essential feature the acquisition of illegal property gain for a legal person or violation of a duty of a legal person, as a legal precondition of criminal responsibility of a legal person for a criminal offence committed by its responsible person; deletion of the legal person from Court Register with no successor, while judicial proceedings are in progress; lack of assets under the legal person's disposition to cover the costs of the proceedings or being subject to bankruptcy proceedings (meaning it is not cost–effective to take action); difficulty in determining the responsible persons actual powers and responsibilities (particularly where there are several). These obstacles to effective enforcement raise attractiveness for abusing legal persons.

[198] Total indictments (no data is available Indictments after investigation/direct indictments).

708. The NRA identified risks related to legal professions (lawyers, notaries, accountants), noting that these provide services of setting up companies, operation or management of trusts, companies, foundations or similar legal arrangements, which increases their risks. At a high level in the NRA, it is indicated that lawyers and notaries may be involved in ML schemes and that accountants may be accomplices in ML schemes. The extent to which these professions may be actively or unknowingly involved in the misuse of legal persons appears to have been qualitatively assessed in the NRA, but no details and substantiation are provided.

709. Since January 2020, foreign trusts or equivalent entities where the trustee resides in Croatia, the trust establishes a business relationship with a RE or buys real estate in Croatia (unless it is registered in another EU Member State) is obliged to have a personal identification number. The authorities suggested that they had no occasion to observe trustee of foreign trusts residing or operating in Croatia. Having a PIN number is a prerequisite in accomplishing the transition for purchase of real estate and when entering into a business relationship with a Croatian RE. The TA confirmed that conducted analysis of the types of organisations holding a PIN number, where no foreign trust was detected. This was also confirmed through analyses of the consolidated bank account register. While this points to a possible absence of foreign non–EU trust activities in Croatia and suggests that associated ML/TF risks in Croatia would be at a lower level, the conducted exercise does not amount to analysis of ML/TF risks related to a foreign trust, and effect of this described new mechanism on mitigation of potential ML/TF risks.

710. It is noted in the 2020 NRA that there is only one company, the activity of which includes among others the provision of fiduciary, office rentals, virtual offices and business address rentals services., but the NRA does not contain an analysis of vulnerabilities of this arrangement.

711. There is a general understanding among the authorities of the types of legal persons that are of higher and lower vulnerability. LLCs, particularly Simple LLCs, are regarded as more vulnerable, and JSC (public companies) and companies with listed shares are generally regarded to be less vulnerable to abuse for ML/TF. This is due to the rules surrounding their establishment and ongoing operation, particularly in terms of share ownership and disclosure, and the frequency of featuring these types of legal persons in STRs and criminal investigations.

712. When discussing the lack of a comprehensive risk assessment of particular types of legal persons on–site, there appeared to be some reluctance as there were concerns with LLCs and SLLCs being designated higher risk. The majority of companies in Croatia are set up in these two forms of private companies (LLCs and SLLCs). 88.2% of all BOs of all legal persons are Croatian nationals. 89.3% of LLCs and 98.7% of SLLCs do not have a complex ownership structure as they are owned by natural persons. The AMLO indicated that many are being used legitimately, with the majority having a simple ownership structure owned by natural persons and it would not be appropriate to designate all LLCs/SLLCs as being at higher risk. Rather, it was proposed to limit the higher risk designation to where there are certain high–risk indicators in line with detected typologies and trends. TA highlighted that in its opinion, vulnerabilities of legal persons are higher in the instances when there is foreign ownership, several persons are registered on the same address and/or one person registers several companies. These, being criteria that are not associated with a certain type of legal person but rather with who is setting up a legal person and how.

**Box N°7.2: Use of LLC and Simple LLC for illegal purposes**[199]

The AMLO analysed the STR from a bank received in 2017. The STR described that over a period of one year, a total of EUR 6 700 000 was transferred to a company LLC 1 (registered in Croatia) to its account in Croatia, from three foreign companies from Country A. This amount was subsequently transferred by LLC 1 to another company in country B.

Analysis of the case revealed that there were also three other companies registered in Croatia involved in the scheme – LLC 2, SLLC 3 and LLC 4. These did not have any business activity or recorded turnover on their Croatian bank accounts but had accounts in the country A and B which were used to transfer funds to these companies.

In addition, Croatia revealed that: (i) 1 out of these 3 companies had the same owner as LLC 1; (ii) 2 out of 4 companies were also founded by a national from country A; and (iii) 3 out of 4 companies mentioned in this case had the same registered address in Croatia. All of these companies were set up via notaries (not online) and the citizens from country A were present in Croatia when founding the companies.

AMLO established that the scheme aimed at covering up VAT fraud and/or abuse of trust in business operations. The case was disclosed to the TA with suspicion of ML and the related predicate tax–criminal offence.

The TA: (i) filed a criminal complaint against LLC 1 (CC, Art.291(1)200); (ii) filed a criminal complaint against LLC 2 (CC, Art.246) and collected EUR2mln. of taxes; (iii) filed a criminal complaint against SLLC 3 (CC, Art.291(1)) and collected EUR2.4mln. of taxes; submitted a misdemeanour indictment against LLC4 (VAT Law, Art.83 and 86). The TA suspended VAT ID numbers of all 4 companies.

713. The authorities independently of each other, demonstrated some understanding of vulnerabilities of legal persons, which were based on observations of their operational practices. However, the large amount of information that is in possession of authorities, as described above, was not consolidated and analysed in a systemic manner to assess the vulnerabilities of various types of legal persons and the extent to which legal persons created or registered in Croatia can or are being misused for ML. No analysis and limited understanding were displayed with respect to legal arrangements operating in Croatia (confined to foreign trusts). TF vulnerabilities of legal persons and arrangements are not explored.

### *7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements*

714. Croatia has in place a range of measures to mitigate the misuse of legal persons and arrangements, such as the requirement to register legal persons and legal arrangements operating in Croatia in various registers (Court Register, Register of Foundations, Register of Foreign Foundations, Register of Associations, Registered of Foreign Associations[201]), where basic information is registered. Recently Croatia set up a BO Register, which became operational

[199] AMLO Annual Report 2018
[200] CC Art.246 "Abuse of Trust in Business Dealings" CC, Art. 291(1) "Abuse of Position and Authority", VAT Law, Art.83 "Bookkeeping obligation" and 86 "Application for acquisition of goods from other EU Member States".
[201] https://registri.uprava.hr/#!uvid

since January 2020. While the BO Register is still relatively new the efforts to fully populate it are encouraging, but the effectiveness of this cannot yet be assessed.

715. Companies and institutions in Croatia must be registered with the Court Register. There are two ways for establishment of companies: one requires the involvement of a Notary Public and the other, which is an on–line registration process, does not. Only the LLCs and Simple LLCs can be established on–line. As of 31 December 2020, there were only 856 companies established using the on–line registration system.

716. As of the date of the on–site, the majority of legal persons were established via applications submitted to the Court Register by Notaries Public. Notaries Public, as part of their role, conduct CDD on the natural persons and legal persons named in the application documents. An application for registration includes specified information for legal persons and the personal identification number (PIN) for natural persons, all witnessed by a notary public. Presentation of identification documents for all natural persons named in the application is required by the Notary Public. Members of the Management Board are required to make a self–declaration that they have no criminal record, on which Notary Public relies and undertakes no verification. No such declaration is required from shareholders, either domestic or foreign. When dealing with foreign natural persons, no certificate of criminal background is obtained. No verification is conducted of the rationale for a natural person to have a role in the legal person (e.g., a frontman (homeless person) can be registered as a shareholder or a member of a management board of a company, effectively acting on behalf of another person). A foreign legal person should present a balance sheet to verify its existence and financial standing. The Court Register conducts a purely administrative process and does not undertake any checks on the natural persons (except for ID) and legal persons disclosed in the application documents. Unless there are irregularities with documents, the legal person will be registered. No further ongoing checks are made to identify the change in the situation of the shareholder and of the management of the legal person.

717. The effect of this mitigating measure, nevertheless, raises doubts for two reasons: the performance of the Notaries and reliance of the Court Register on the Notary to verify the submitted information for registration. The supervisory inspections revealed numerous irregularities in the performance of the Notaries with respect to collection and verification of data. Among these, failure to collect appropriate information on the person or to identify the BO information from an authenticated source. The Notaries, as also mentioned above, are filing a very low number of STRs, which does not match with expectations, considering the level of exposure of the legal persons to criminal abuse. In addition, the Notaries Public are of the opinion that the Court Register conducts checks and verifications of submitted data, hence any irregularity would be communicated back immediately. The Court Register highlighted that it would proceed with registration except for where there is outstanding information that would raise a need to verify submitted documents. Therefore, the effectiveness of the mitigating measures here is affected by the mutual reliance on the quality of each other's performance by the Notaries Public and the Court Register, as checks and controls that form the basis of this registration mechanism are not enforced.

718. The LLCs and Simple LLCs can be set up online through the START system[202]. Only natural persons can set up these types of legal persons online. There are also no legal persons or arrangements permitted in the ownership of the entities registered online. Also, legal persons are

[202] Start (gov.hr)

not permitted to be members of the management or supervisory boards (directors) in Croatia[203]. As compared to the registration process described above, this system does not mandatorily involve a Notary Public, hence no CDD or verification is conducted by a "gatekeeper". Checks in place include verification of the identity of founders and shareholders through the ID card of a natural person using the National Identification and Authentication System (NIAS[204]). Reliance is placed on a self–declaration regarding the absence of criminal convictions with no verification mechanism applied. No ongoing monitoring and verification of information is in place. There is a high degree of reliance on the legal obligation of the authorised person (e.g., members of the management board) of the legal person to ensure that truthful information is provided, and all the changes in the situation of managers or shareholders are reported accurately and timely with no operational mechanisms for checks and controls by authorities.

719. Foundations and Associations (on a voluntary basis) are registered by the administrative body of the counties or the City of Zagreb, according to the seat of the association or foundation, and upon registration included into the Register of Foundations and Register of Associations. There are similar mechanisms also applied for registration of foreign foundations and associations. There is no online registration mechanism available for foundations and associations. The registration process includes verification of the identity of the founders, the management body and the liquidator. No criminal background checks are performed. No checks are conducted against UN TFS. No mechanism is in place for verification of information and ongoing monitoring of any changes in foundations and associations. Reliance is placed on the authorised person of foundation or association respectively to provide timely information on any change of the respective persons. The involvement of the Notary Public is not a prerequisite in this process.

720. Overall, lack of criminal background checks, insufficient application of checks and controls in the registration process, lack of ongoing monitoring and verification of information constitute weaknesses in the described mitigating measures.

721. There is no statutory requirement for Companies, foundations or associations to have a bank account when established. Nevertheless, unlike foundation or association, when it comes to Companies, in the registration process, they would have to provide the paid–up share capital, and hence, in practice, need to have a bank account. Therefore, it will be subject to CDD checks of the bank (who acts as an informal "gatekeeper") at the initial stage of formation. This would ensure that if the legal person or any related person are listed in the UN TFS, these will be detected. Nevertheless, this does not ensure that criminals subsequently would be prevented from being a manager, shareholder of a BO of a Company. It was not clear that the company's funds had to be held in a Croatian bank. No data was available on how many legal persons had non–Croatian bank accounts.

722. Despite legal persons, especially LLCs and Simple LLCs, frequently featuring in STRs, the authorities suggested that from 2015 to 2020, there were no STRs filed by the banks with suspicions raised when the legal person was opening an account as part of the registration process.

723. As was indicated above, recently, aimed at enhancing transparency of legal persons and arrangements, Croatia has introduced a new mechanism – a BO Register. The Financial Agency is responsible for establishment, maintaining and management of the BO Register on behalf of the

[203] Article 239(2) and 255(1) plus 436(1) of the Croatian Companies Law
[204] NIAS (gov.hr)

MoF. Croatia has to be commended on its efforts undertaken to implement and populate the BO Register. This Register is set to keep BO information on all types of legal persons set up in Croatia (except for ones that are listed on the stock exchange) and trusts and similar entities of foreign law. Unlike domestic ones, foreign foundations and foreign associations are not required to register in the BO Register.

724. Authorities suggested that as of 1 May 2021, 15 518 records were outstanding, relating to 8.2% of all entities. The majority of the entries related to LLCs (6 682) and Simple LLCs (7 076). While Croatia initially was aiming at completely populating the BO Register by 31 December 2019, COVID–19 related restrictions considerably slowed down the process. While unregistered BO information on 13 758 LLCs and Simple LLCs raises concerns in the light of the scale of misuse of these types of legal persons, the Croatian authorities stated that they keep populating the BO Register.

725. The Finance Agency indicated that despite the deadline for the registration of the BO information having passed, there is currently a moratorium on the application of misdemeanour proceedings for failing to populate the BO register or update it, due to the COVID–19 pandemic. This moratorium is applied with no defined deadline and would be lifted when the situation with the COVID–19 pandemic changes. This decision does not define any criteria suggesting the change in situation which would terminate the moratorium. Therefore, this raises concerns with the application of a moratorium with an undefined deadline.

726. It is the responsibility of the legal person via their authorised person to initiate registration with the BO Register after being set up and registered with the respective authority. At the time of the on–site, there was no mechanism in place for informing the BO Register about new entries (registration of or change in the legal person or arrangement). Hence, the BO Register would know about the new entry only when approached by the legal person, which is a gap in the system.

727. When a legal person submits the information required to BO Register, the Finance Agency checks (i) the identity of the person indicated as a BO using the Central Personal Identification Number Application System maintained by the TA; and (ii) the fact of the legal person being registered in the Court Register, register of associations or foundations respectively. No checks are undertaken on the accuracy of the BO information, criminal background, against UN TFS or adverse intelligence. The TA conducts some checks when doing tax investigations.

728. Overall, the gap in communication between various registers and a BO Register for prompt information exchange on a new entry, postponement of application of sanctions for late submission of information to the BO Register, lack of criminal background checks, and verification against UN TFS or adverse intelligence constitute weaknesses of the mitigation system through the BO registration mechanism in Croatia.

729. The BO Register should contain data on the BO of trusts who have a Croatian Trustee or who forms a business relationship with a RE or purchases Croatian real estate (if it does not have a registration in another EU–members state). No such entities were registered with the BO Registry at the time of the on–site. The private sector and the competent authorities suggested that foreign trusts are rare in Croatia, with only a couple of examples of participating in ownership structures.

730. When forming a secret society, this agreement should be filed with the TA, either by the Notary Public (if one was involved) or by the entrepreneur. If such arrangement results in the secret member acquiring a BO interest in the company, this information should be submitted to the BO Register. If it constitutes an entrepreneurial contract, it would need to be registered with

the Court Registry. However, there are no specific checks made on the parties involved in the secret society from the perspective of prevention of misuse of this arrangement for criminal purposes. There are also no mechanisms for active detection of such arrangements if not reported by the parties to the arrangement. Such information may come to the authorities' attention when there is a dispute between the parties which is filed with the Court.

731. Bearer shares can no longer be issued by JSC. According to data from the central securities depository, 5 JSCs issued bearer shares out of a total of 690 JSCs. Those 5 companies have issued a total of 330 832 874 shares, 66 023 of which are bearer shares. No data is available on how many of these have been converted into registered shares. Under the current legal provisions, bearer shares cannot be transferred, exercise any rights attaching to them, such as the right to vote or be traded without the holder of the bearer shares notifying the company of their identity and proving ownership. There is still a risk that the small number of bearer shares may be held by criminals, but to gain any benefit from the bearer shares, their identity would have to be ascertained, so while not a complete ban, it does provide effective mitigation.

732. Nominee shareholders and nominee directors are not concepts recognised by Croatian law. The NRA describes homeless and disabled persons as being frontman, and in most of these cases, effectively, these persons were acting as shareholders and directors on behalf of others. The authorities advised that there is no difference in the types of directors in Croatia. Every named director will be held liable if their fiduciary duties are neglected. However, this would not prevent the existence of arrangements whereby one natural person formally acts as a director on behalf of another person, although the authorities indicated that this would be illegal.

733. There are no mechanisms for systematic monitoring of instances when legal persons or arrangements are set up at the same address, by the same person, have the same manager, BO, etc. The Registers did not demonstrate awareness of such instances and, were unable to estimate how often they occurred in quantitative and qualitative terms or that they had any mitigating measures in place. The TA suggested that it takes into consideration the number of entities registered at the same address when conducting a risk analysis of taxpayer – legal persons.

734. Reference was made in the on–site to websites offering to establish companies and provide shelf companies. Authorities described how these had been investigated and that they were not in reality capable of offering these services. In the view of authorities, legislative requirements on notification of changes of ownership and sales/transfers of companies to the Court Registry should not allow for the use of shelf companies without the BOs and controllers being also disclosed to the BO Register. Nevertheless, the obligation is on the authorised person of legal person to notify of the changes to the company, and there is no active supervision of this requirement.

735. While no risk assessment has been undertaken in relation to misuse of inactive/passive entities from the public registers, it is apparent that Croatia regularly strikes off dormant entities. This also ensures the accuracy of the Companies Register, the Registers of domestic and foreign Associations and Foundations. It is noted, however, that there are some issues with striking off the NPOs (see IO.10). In 2018–2020 there were respectively around 4 300 companies deleted ex officio (company did not publish its annual financial report for 3 years), 4 600 Associations and 25 foundations deleted by a court decision (on the completion of insolvency proceedings), 5 foreign associations and 1 foundation deleted (discontinued operation in Croatia).

### *7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons*

736. In Croatia, basic and BO information is obtained from multiple sources: the Registries, REs, directly from the legal person, a TA database of legal persons, or foreign partners, when necessary (see IO.2).

737. Basic and BO information is available to all competent authorities through various registers of legal persons, which are accessible online for no fee. Discussions with the LEAs, AMLO and supervisory authorities revealed no difficulties accessing the basic information on registered legal persons either through online mechanisms or through direct co–operation with the Registers. The LEAs indicated that they do not use the BO Register, which was mainly due to the recent nature of this register, its ongoing population and pre–existing established working practices of the LEAs for obtaining such information through their own channels.

*Access to Court Register information*

738. Information kept with the Court Register is accessible to any counterpart from the website instantaneously[205]. It includes information on the legal person, such as PIN, title, legal form, subject of business, address, share capital and every change, shareholders, supervisory board, authorised person, statutory changes, links to financial reports for the last two years. The website also contains information about terminated legal persons. The officially certified extract from the register can be obtained directly from the website, which is valid for 3 months. Competent authorities can easily obtain all this information and a paper copy of ID documents free of charge upon a formal request. As described above, there is a multistep system of registration of legal persons designed in Croatia to have a system of checks and controls, but the assessment team observed a high level of mutual reliance demonstrated by the Court Register and the Notaries Public. This raises doubts about the adequacy and accuracy of the available information.

739. There are less stringent mechanisms in place for verification timeliness, of provided information when registered on–line, except for the instances when the ID document of a natural person expires. Adequacy of information is ensured through the mechanisms in the electronic registration system, which would require having all the mandatory fields filled in. Accuracy of the provided information is verified through NIAS – ID data verification system. No Notary Public involvement is required.

740. Legislation requires notification of changes of basic information and shareholdings to the commercial court within 15 days of the change, but this is not subject to supervisory checks by the Court Register. Save for where the authorised person's ID documents expire. There appears to be over–reliance on self–reporting of changes with little effective monitoring or checking to ensure the register is updated in a timely manner. In the absence of information on detected non–reporting of changes and with a lack of data regarding the application of sanctions, the accuracy of the registers cannot be verified and confirmed.

*Access to information on JSCs*

741. Information on holders of dematerialised shares is retained by the Central Depository & Clearing Company Inc. (CDCC). CDCC operates as a central securities depository and a registry of dematerialised securities, where data on issuers, securities, securities accounts, securities holders and other legally required data is kept in the form of electronic records. The top 10

[205] https://sudreg.pravosudje.hr/registar/f?p=150:1, https://registri.uprava.hr/#!udruge

accounts with the most shares (top 10 shareholders) of every security (share) are publicly available by accessing the CDCC website. AMLO, SAO, Police and the CFSSA for supervisory purposes access the CDCC's records when necessary.

*Access to Foundations Register, Foreign Foundation Register, Register of Associations and Register of Foreign Associations information*

742. Information kept with the Foundation Register, Foreign Foundation Register, Register of Associations and Foreign Associations is publicly accessible from the website easily[206]. The registers contain the following core information on foundation/association, including the PIN, title, status, date of setup, address. For foundations, information is held on: authorised representatives, members of the governing body, purpose, basic assets (not always is filled out), founding documents. The register of associations includes information on the assembly of association, authorised representatives and duration of their terms, liquidators, goals and activities (including economic), statute (with amendments if occurred). Similar information is held for a foreign association except for assembly of association, liquidators, and statute. If the foundation or association, domestic or foreign, is registered as NPO, it is indicated and a link to the database provided. In case the foundation/association ceases to exist, the database provides references to the relevant administrative decisions (also information on the liquidator of an association) and the date of termination on activities. This data is also easily accessible. All the data contained in the register, including the copies of ID and other documents, are available to competent authorities upon request.

743. As concerns the accuracy and timeliness of changes to the register, in the absence of information on detected non–reporting of changes, the accuracy of the registers cannot be verified and confirmed.

*Access to BO Register information*

744. The competent authorities of Croatia have direct access to the BO Register, with advanced search tools available to them.

745. As concerns the adequacy, accuracy and timeliness of information reflected in the BO Register, the assessment team could not reach a conclusion due to the very recent nature of the Register and absence of adequate information on conducted checks of available information. As was mentioned above, the BO Register was yet to be fully populated.

746. The responsibility for updating information on BO and any further changes in the legal person, at a legislative level, is the obligation of the authorised person of legal person or arrangement. The BO Register informed that collecting BO information from legal persons is challenging as they often mix the concept of BO with direct ownership or shareholding. In these cases, explanations are provided by the BO Register and information is corrected.

747. The TA indicates that when conducting tax supervision of legal persons, they check all the BO data provided and also whether there are secret society arrangements. BO information can also be checked upon a RE notifying the AMLO about discrepancies, which is also forwarded to the TA. If information were submitted to the TA that indicated irregularities in the BO database, they would initiate an inspection of the legal person or arrangement.

748. The TA suggested that whenever conducting inspections, they would have always looked at all documents regarding legal persons or arrangements. Since January 2020, they have had

[206] https://registri.uprava.hr/#!uvid and https://registri.uprava.hr/#!uvid

additional powers with respect to BO data verification. It was stated that since then, verification of BO data became a separate item of inspection, and if issues are revealed, these would be reflected in the inspection report. Due to the recent nature of this change, no information was yet available on the inspections and the accuracy of BO Register information.

749. The ability of the authorities to obtain information in a timely manner about how the BO of legal persons may be influenced by the existence of secret society contracts was cast into doubt by information provided post the on–site. It was confirmed that the TA had registered 21 secret society contracts and in 5 contracts, the secret members could be considered BOs. 4 of the 5 secret members were not registered in the BO Register. There are no mechanisms for active detection of such arrangements if not reported by the parties to the arrangement.

750. The TA informed that drafting of a Guidelines for supervision of persons obliged to enter information in the BO Register was underway during the on–site. This will be followed by Instructions on supervision procedure over the entry, updating and accuracy of the data entered into the BO Register, and the TA will carry out the supervision of the data entered into the Register based on this document.

751. There is a requirement for REs to notify the AMLO if there is any discrepancy detected in relation to BO information held and data provided in the BO Register. This should be done after the RE has verified the BO information from its own data and other independent sources. The private sector indicated they had on occasions submitted notifications to AMLO for further correction of data. The AMLO reports that 6 banks have reported 45 discrepancies in BO data. None of these triggered dissemination to the TA for further action. Involvement of REs in verification of BO information provides a useful cross check of the BO data maintained with the Register but does not compensate for the lack of checks and proactive supervision.

752. Overall, this convoluted multistep process for verifying and subsequent correction of the BO Register information. While this has not been fully tested, in practice, it does not seem to ensure promptness of the process. It requires that: (i) REs verify their own data with the BO Register and independent reliable sources; (ii) report any discrepancies to the AMLO; (iii) the AMLO conduct additional checks on the received notifications; (iv) if confirmed they submit the notification to TA (for action) and Finance Agency (for information); (v) the TA conduct an inspection; (vi) if a discrepancy is revealed they order corrections to be made to the BO Register; (vii) and report the matter to the Financial Inspectorate to institute misdemeanour provisions.

*Access from other sources*

753. Competent authorities also rely on other sources of information on basic and BO information of legal persons, such as TA database, REs and legal persons, directly.

754. The database of the TA is consulted by the competent authorities occasionally to obtain information. Among others, this database contains information on authorised persons, shareholders and BOs of companies, secret societies, bookkeeping services, employees. Co–operation between the competent authorities takes place smoothly and timely.

755. As concerns secret society, no data or statistics for the number of secret societies filed with the TA was provided on–site. Post the on–site Croatia confirmed that the TA had received 21 secret society contracts and in 5 contracts the secret members could be considered beneficial owners. 4 of those 5 secret members were not registered in the BO Register. Hence, timely access to relevant information about these arrangements and its quality is questionable.

756. REs constitute another useful source of basic and BO information. REs provide information on legal entities to the AMLO upon request and as part of STRs. LEAs can also obtain this information directly from REs by warrant or court order (which stipulate timeframes) or through co–operation with AMLO. Supervisors, when necessary, obtain BO and basic information on legal entities from REs as part of their supervisory activities.

757. Where necessary, in the course of criminal proceedings or a tax audit, the LEAs and TA obtain basic and BO information directly from the legal persons.

758. The representatives of various competent authorities noted that they never encountered any difficulties or delays obtaining basic and BO information from either of the mentioned sources. While authorities do not maintain statistics on the timeliness of access to data, they have suggested obtaining data from the private sector ranging from within 1 hour to 5–8 days maximum. The evaluation team also did not come across adverse information when discussing criminal cases, STRs or supervisory efforts.

### *7.2.5. Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements*

759. According to the Croatian authorities, there are no types of legal arrangements that can be established in Croatia. Information regarding foreign non–EU registered trusts would be accessible for competent authorities from the BO Register. Information on EU registered trust would be accessible from the REs serving the former as a customer or from a foreign EU Member State counterpart. No cases were highlighted concerning legal arrangements being specifically brought to the attention of the AMLO. LEAs would seek information the same way they access information for legal persons. As concerns the supervisors, all data is available to them when dealing with REs while conducting inspections or gathering information for off–site monitoring.

760. Trustees are designated as a type of RE that should be supervised by the Financial Inspectorate. When detected and engaged with the Financial Inspectorate, the latter would be an additional source of timely access to information on trusts.

761. Trustees and other types of REs are required to have appropriate, accurate and updated information on the BOs of the trust (i.e., settlor(s), trustee(s), protector(s), beneficiaries, persons performing similar functions in the case of other legal arrangements, and other persons who exercise control over the trust). The only TCSP primary business known to the Financial Inspectorate provides services to companies, not trusts.

762. Full information should be sought by a RE when trust acts as a customer. So far, no foreign trusts are recognised by anyone interviewed as operating in Croatia save for a couple of interviewees referring to the fact there was a foreign trust in ownership structures of their customers. Save for 1 accountant those (who does provide company services), other accountants and lawyers confirmed they had not come across trusts in their practice. Notaries who are responsible for setting up most forms of companies also indicated they were not aware of trust activity in Croatia.

### *7.2.6. Effectiveness, proportionality and dissuasiveness of sanctions*

763. Croatia could provide no appropriate information on application of sanctions to comprehensively analyse the system and applied practices and to conclude that the framework is effective.

764. There are over 170 000 registered legal persons in Croatia. No qualitative or quantitative data was provided for failing to provide accurate basic information or shareholding information for legal persons or the level of any actual sanctions imposed. Penalty charge notices for late notification of information, not within the prescribed time limits, were imposed by the Court Register: 43 931 in 2016; 41 279 in 2017 and 28 961 in 2018. No data is available for 2019 and 2020, so the AT is unable to assess whether the reduction in penalties demonstrates the effectiveness of this measure.

765. Information on rejected applications for the Registers of Associations and Foundations was provided, with reasons for rejections are stated as follows: applications were not in accordance with law or statute of the association/foundation, and evidence was omitted, and deadlines were exceeded. No financial penalties imposed were made available. As concerns rejected applications for Registers of Foreign Associations, there was only one occasion[207] in 2017 and no instances for Foreign Foundations.

**Table 7.2: Rejected change applications for Associations and Foundations**

| Register of Associations | | | | | | | Register of Foundations | |
|---|---|---|---|---|---|---|---|---|
| **Year** | **2015** | **2016** | **2017** | **2018** | **2019** | **2020** | **2019** | **2020** |
| Number of rejected applications for entry | 23 | 19 | 15 | 25 | 32 | 24 | 1 | 4 |
| Number of rejected applications for entry of changes | 182 | 111 | 86 | 83 | 118 | 65 | 1 | 0 |
| Number of dismissed applications for entry of changes | 81 | 41 | 35 | 39 | 44 | 45 | 0 | 0 |

766. No sanctions are currently being imposed for failures to populate information (deadline was 31 December 2019) or notify of changes to information in the BO register (within 30 days of change) as a result of the moratorium applied Finance Agency.

767. The TA indicated that if they found irregularities in the BO data in the BO Register during the course of their tax investigations, they would file a misdemeanour complaint. Fines range from EUR 670 up to EUR 100 000 for the most severe demeanours. These sanctions are seen to be adequate if applied proportionately to detected irregularities to have a dissuasive effect.

### *Overall conclusions on IO.5*

768. The authorities, independently of each other, demonstrated some understanding of vulnerabilities of legal persons, which were based on observations of their operational practices. However, a large amount of information in their possession was not consolidated and analysed in a systemic manner to assess the vulnerabilities of various types of legal persons and the extent to which legal persons created or registered in Croatia can or are being misused for ML. No analysis and limited understanding were displayed with respect to legal arrangements (confined to foreign trusts) operating in Croatia. TF vulnerabilities of legal persons and arrangements are not explored.

[207] Association Law, Art 26 "The request for entry in the register of associations shall be rejected if the statute determines the goals and activities of the association in conflict with the Constitution or the law".

769. In Croatia, all registers are accessible online, which makes publicly available basic, shareholding and BO information on legal persons and arrangements. There are some issues that affect the transparency of legal persons and prevention of their misuse. These are due to deficiencies such as the lack of criminal background checks of respective persons and verification of information, mutual reliance of authorities involved in the process of incorporation of legal persons, lack of monitoring of changes and supervision over the overall process. This also prevents the information from being accurate and current in all instances. Lack of information on the application of sanctions for non–compliance with information requirements prevent the AT from concluding the system is effective. No indications were identified that access to information on basic and BO information is not timely.

770. Overall, although the ML abuse of legal persons is widespread in Croatia, taking into consideration the context of the country, which is not of major regional importance in terms of its economy and trade, major improvements are needed to improve the system.

771. **Croatia is rated as having a Moderate level of effectiveness for IO.5.**

# 8. INTERNATIONAL CO–OPERATION

## 8.1. Key Findings and Recommended Actions

***Key Findings***

***Immediate Outcome 2***

a) Croatia provides constructive assistance in the field of MLA and extradition in relation to ML, predicate offences (except for the fiscal offences when dealing with non–EU Member States), and TF. In practice, the co–operation is conducted primarily with countries in close vicinity. This is supported by a network of multilateral and bilateral agreements. Assistance is also provided on the basis of reciprocity.

b) In practice, since 2017, incoming and outgoing requests with non–EU Member States are sent through the MoJA, and with EU Member States, it is done through SAO. There was no major issue in international co–operation through either of the mechanisms, but occasional delays are observed when requests are sent through the MoJA. Neither the MoJA nor the SAO disposes of prioritisation mechanisms.

c) Croatia is seeking foreign co–operation to a limited extent only. Limited appreciation of ML offence (see IO.7) by the Croatian authorities affects outgoing MLA and extradition requests. Given the risk profile of the country and its exposure to broader international threats, this posture might lead the country to miss opportunities for identifying and investigating relevant cases.

d) Throughout the whole reporting period, the outgoing requests on freezing and confiscation of assets remained modest, which is inconsistent with Croatia's geographical exposure to ML and predicate offences (see IO.8).

e) A significant number of outgoing MLA and extradition requests are refused by foreign counterparts. The country has not taken a systematic approach to identify and eliminate the underlying systemic issues behind it.

f) Informal co–operation represents a strong side of the system. Nevertheless, it is unclear to what extent LEAs and the AMLO systematically disseminate the relevant information to their foreign counterparts spontaneously.

g) The supervisory authorities demonstrated a relatively good level of international co–operation. Nevertheless, the TA lacks a designated legal framework and channels for information exchange in its capacity of AML/CFT supervisor of games of chance.

h) When requested, Croatia provides information on basic and BO of legal persons. The international co–operation feedback did not indicate any specific issue linked to the quality of co–operation provided by the Croatian authorities. The issues highlighted in IO.5 can have an impact on the accuracy of the information.

***Recommended Actions***

***Immediate Outcome 2***

a) Croatia should introduce as a policy objective systematically seeking international co–operation when investigating criminal cases of ML, associated predicate offences or TF with a foreign element. Assistance should be pursued in line with its risk profile. Particular attention should be given to freezing, seizure and confiscation of assets moved abroad in all relevant cases.

b) Croatia should analyse cases of refusal of its outgoing requests, taking appropriate actions to identify and eliminate the systemic issues that prevent constructive international co–operation.

c) Croatia should develop guidelines for prioritisation of the AML/CFT requests received through all relevant channels and ensure that the case management systems for MLA and extradition requests and procedures are harmonised with deadlines provided to guide authorities.

d) LEAs and the AMLO should systematically consider disseminating the relevant information to their foreign counterparts spontaneously.

e) The TA, in its capacity as a supervisor over games of chance, shall be provided with adequate legal instruments and communication channels to secure AML/CFT international co–operation in all relevant instances.

f) Croatia should consider widening the scope and subject matter of existing bilateral agreements, ensuring the use of the most efficient channels of communication in the area of MLA.

772. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36–40 and elements of R.9, 15, 24, 25 and 32.

## 8.2. Immediate Outcome 2 (International Co–operation)

773. International co–operation is an important part of the Croatian AML/CFT regime given its risk profile and geographical position as a transit country on the so–called "Balkan route". This exposes Croatia to an increased ML risk. Most co–operation is undertaken with neighbouring EU and non–EU Member States.

### *8.2.1. Providing constructive and timely MLA and extradition*

774. Croatia has in place a satisfactory legal framework to provide MLA and extradition, including multilateral treaties and bilateral agreements. Croatia provides a wide range of assistance on the basis of reciprocity.

775. The MoJA is the central authority responsible for receiving MLA and extradition requests and transmitting them to domestic judicial authorities for execution. Until the beginning of 2018, the MoJA was responsible for communicating with both EU and non–EU Member States for the purpose of MLA co–operation. Following the fully–fledged implementation of the European Investigation Order (EIO) Directive in December 2017, the SAO became responsible for receiving

all requests issued by EU Member States except for taking over the criminal proceedings. Since then, the MoJA has been responsible for judicial co–operation strictly with non–EU Member States.

*MLA*

776. In the MoJA, there are currently 13 employees in the Sector for MLA. Once an MLA request is received, it is assigned to an employee of this sector, who then marks various categories in the system (the criminal offence is in question, the requesting country, the type of MLA requested). The authorities confirmed that the statistics collected do not include data on the requests for judicial co–operation submitted directly to the relevant Courts.

777. Croatian authorities receive incoming requests mostly from neighbouring EU and non–EU countries, which correlates with the risk profile and context of the jurisdiction. Within the whole reporting period, there were 13 ML–related incoming requests received through the MoJA, executed from 30 to up to 300 days (see table 8.1). The timing of execution depended on the substance of the specific request and the actions required to be taken. Overall, most of the requests were executed within the shorter average of time, with only a few taking longer. The number of incoming requests on predicate offences has been higher – 324 in total, with a significant decrease in the incoming requests since 2017. This is attributed to the switch of competences to the SAO (see table 8.2). The average time for executing an MLA request on predicate offences is 88 days (see Table 8.4) co–operation.

778. The MoJA uses an electronic case–management system (ILA) to monitor the execution of incoming requests. However, it does not have a written prioritisation mechanism. The authorities explained that MLA requests are always considered for urgent execution, yet the average time of execution varies depending on: (i) the type and complexity of the MLA request; (ii) competent bodies involved in its execution; and (iii) possible additional information sought. In practice, when considering the priority of requests, the authorities take into consideration: (i) the deadlines indicated; (ii) whether the request relates to deprivation of liberty; (iii) the need for urgent actions, such as the seizure of assets; (iv) the type of assistance; (v) the type of criminal offence. No specific priority is given to requests dealing with areas of higher risk, which could potentially lead to failure to provide timely assistance for the most significant offences. This, in the view of the AT, constitutes a severe deficiency.

779. In 2019 and 2020, the rate of predicate–related incoming requests refusals has reached around 15%. The authorities explained that these refusals are beyond the country's control (e.g., addressee is dead or could not be located). Yet, Croatia did not analyse the exact reasons for refusals, and no efforts were taken to minimise the increasing share of requests not executed by competent authorities when communicating with both EU and non–EU States.

780. Although the legislation does not allow Croatia to provide MLA to non–EU Member States on fiscal offences (see R.37), the AT examined the refusals over the period, and no requests were refused because of this legislative limitation. Therefore, while the concern remains, this did not have any material impact on MLA provided by Croatia during the assessed period.

**Table 8.1: Incoming requests on ML addressed to the MoJA**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | Total |
|---|---|---|---|---|---|---|---|
| Received | 3 | 1 | 1 | 3 | 3 | 2 | **13** |
| Executed | 3 | 1 | 1 | 3 | 3 | 2 | **13** |

**Table 8.2: Incoming requests on predicate offences addressed to the MoJA**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | Total |
|---|---|---|---|---|---|---|---|
| Received | 108 | 80 | 47 | 46 | 30 | 13 | **324** |
| Executed | 100 | 75 | 44 | 44 | 26 | 11 | **300** |
| Refused | 8 | 5 | 3 | 2 | 4 | 2 | **24** |

781. As previously indicated, since 2017, the SAO has carrie out extensive co–operation via EIO. This represents a significant part of Croatia's MLA co–operation. To further facilitate international co–operation within the EU, Croatia uses different EU instruments of direct co–operation such as EUROJUST and the European Judicial Network in Criminal Matters (EJN). They have appointed 27 contact persons under the EJN to provide efficient co–operation with their EU counterparts.

782. The Croatian authorities have also concluded agreements on direct prosecutorial co–operation with their principal non–EU Member States counterparts[208]. This facilitates bilateral co–operation and takes on board the specific national peculiarities of the relevant counterparts for taking over proceedings for serious crimes and transnational organised crimes.

783. The SAO applies a case tracking system (CTS) to support the work of Criminal Departments (State Attorneys) and monitor the status of the incoming requests. However, this mechanism does not ensure their prioritisation, which might potentially affect the timely execution of the requests. Over the reporting period, the SAO received 12 ILA requests and 73 EIO dealing with ML (see table 8.3). Requests on predicate offences (see table 8.4) reached 49 ILA and 178 EIOs starting from 2018 per year on average.

**Table 8.3: Incoming requests on ML addressed to the SAO**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO |
| Received | 4 | – | 1 | 1 | 1 | – | 1 | 20 | 3 | 30 | 2 | 22 |
| Executed | 4 | – | 1 | 1 | 1 | – | 1 | 20 | 3 | 29 | 1 | 21 |
| Refused | – | – | – | | – | – | – | – | – | 1 | 1 | 1 |
| Approx. time | 9 | – | 3 | 11 | 97 | – | 117 | N/a | 60 | 186 | 130 | 25 |

**Table 8.4: Incoming requests on predicate offences addressed to the SAO**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO |
| Received | 49 | – | 54 | 1 | 45 | 10 | 51 | 119 | 42 | 173 | 50 | 243 |
| Executed | 42 | – | 44 | 2 | 27 | 10 | 37 | 185 | 33 | 140 | 37 | 219 |

[208] With Albania, Bosnia & Herzegovina, Canada, Chile, China, Egypt, Kosovo*, Montenegro, North Macedonia, Serbia, South Korea, Ukraine.

* All references to Kosovo, whether the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Refused | 7 | – | 10 | 1 | 18 | – | 14 | 20 | 9 | 32 | 13 | 24 |
| Approx. time | 55 | n/a | 167 | 11 | 70 | 38 | 68 | 68 | 89 | 72 | 81 | 59 |

784. The statistics provided demonstrate an increasing trend in requesting assistance from Croatia for both ML and predicate offences. The time is taken for executing requests received via SAO varies, but overall is adequate. The authorities indicated that most incoming requests deal with fraud and robbery, and to a lesser extent ML, followed by illegal drug trafficking, participation in OCGs and human trafficking. This is to some extent consistent with the ML risk, including its geographical exposure. Most of the requests[209] are come from neighbouring countries, primarily Bosnia and Herzegovina and Serbia, followed by Austria, Slovenia and other EU countries.

785. Throughout the whole reporting period, the Croatian authorities have received in total eight requests dealing with terrorism and six with TF. The country did not face any particular challenges in their execution.

786. Croatia's legal framework allows for co–operation on asset identification, seizure and confiscation. The number of such incoming requests has been sporadic in recent years. Limited information was provided to confirm their execution. No information was provided for the year 2020 and on the search of assets from non–EU Member States.

**Table 8.5: Incoming requests through SAO (ILA or EIO) on search of proceeds of crime**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** |
| ML | – | – | 1 | – | – | – | – | – | – | 28 |
| Predicates | – | – | 4 | – | 3 | – | 1 | 63 | – | – |

787. On the other hand, freezing orders show a stable tendency: four per year for ML and two per year for associated predicate offences on average. In total, Croatia received 23 freezing orders related to ML, out of which five were refused and 13 related to associated predicate offences. Croatia received two confiscation orders relating to ML and four relating to associated predicate offences, which were successfully executed (see IO.8). No requests for search, freezing or confiscation were related to the TF offence.

788. As indicated in R.38, the seizure and confiscation of assets are governed in Croatia by the EU specific legislation, as well as a number of multilateral conventions[210], including the Warsaw Convention (for non–EU Member States). During the reporting period, its foreign counterparts resorted to this instrument four times. This convention provides for confiscation and sharing of property on the basis of recognition and execution of the court decisions of interested parties. In practice, the relevant co–operation requires the conclusion of the country–specific bilateral agreement aimed at securing priority sharing of confiscated property for the purpose of returning

[209] Note: as indicated by the authorities, the numbers provided above do not reflect the exact number of requests sent by the counterparts as they apply different channels of co–operation in the area on MLA. This includes EJN channels, the Eurojust channel, co–operation with specific county Courts.

[210] UN Convention on Corruption 2005, UN Convention on Transnational Organized Crime from 2000, European Convention on Laundering, Search, Seizure and Confiscation of Property proceeds of crime and terrorist financing from 2005, etc.

such property to the legitimate owner[211]. The authorities were not in the position to describe outcomes of applying the Warsaw Convention. Only one case example was provided (see IO.7).

789. Although not exhaustive and lacking input from some close counterparts, international co–operation feedback acknowledges that Croatia's response to MLA requests is in most cases useful and of good quality. In isolated instances, issues on the timeliness and the comprehensiveness of the responses were mentioned.

*Extradition*

790. Concerning extradition, the existing national legislation forbids extradition of nationals to another state, except if made in accordance with the acquis Communautaire of the EU or a bilateral agreement (see R.39). As a central authority, the MoJA is responsible for issuing a decision on allowing the surrender (EAW) or extradition (EXT) of the aforementioned person (under non–EU member request), issuing the decision on transit of the extradited person through the territory of Croatia or giving consent to the transfer of the convicted person, with prior opinion of the SAO.

791. Croatia concluded several bilateral agreements with neighbouring countries which prescribe the procedure for extradition of its own nationals[212]. The grounds for extradition to the aforementioned jurisdictions are in particular: criminal offences committed by a criminal association, corruption and ML offences. Nevertheless, some of these bilateral agreements have a limited application timeframe (e.g., the agreement with Bosnia and Herzegovina) or a limited list of applicable offences. The Croatian authorities were able to demonstrate effective extradition with neighbouring countries sharing close historical ties, even with respect to dual citizenship. In cases when the extradition could not take place, the taking over of the criminal investigation was performed if the relevant evidences were provided to the Croatian side. The country could not elaborate on the exact number of such instances.

792. According to the statistics provided throughout the reporting period, there were eight incoming extradition requests with respect to ML and 521 requests related to predicate offences. No extradition requests were received for TF. The time of execution of these requests varies from five to 228 days. Although the country indicated that all extradition cases were always transmitted as a matter of priority, the lack of a formal prioritisation mechanism may pose complications, in practice. This is due to the fact that: (i) the number of received requests on predicate offences has significantly increased over the reporting period, and (ii) unlike the EU framework (60 days after the arrest of the person), consideration of non–EU Member States extradition requests does not have explicit deadlines.

793. There was never a case of refusal of ML–related extradition request. However, the refusal rate of extradition requests relating to predicate offences increases over the period, namely for the EAW (from 8% in 2015 to 14% in 2020). The authorities indicated that the most common grounds for refusal of an extradition request were: (i) the absence of the accused person in Croatia, (ii) the withdrawal of the request by the issuing State; (iii) failure to meet the double criminality requirement; (iv) the proceedings being already initiated in Croatia. The authorities advised that the drop in numbers in 2020 is attributed to measures taken within the scope of COVID–19.

[211] Croatia was found non–compliant with Art.25(2) in 2016.
[212] Bosnia & Herzegovina (2012), Montenegro (2010), North Macedonia (2011), Serbia (2010).

**Table 8.6: Incoming extradition requests on ML and predicate offences**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **EAW** | **EXT** | **EAW** | **EXT** | **EAW** | **EXT** | **EAW** | **EXT** | **EAW** | **EXT** | **EAW** | **EXT** |
| Received | 40(1)[213] | 14 | 66 | 23(1) | 83(1) | 15 | 77(1) | 12 | 110(2) | 18(1) | 71(1) | No data |
| Executed | 37(1) | 13 | 63 | 20(1) | 79(1) | 11 | 69(1) | 8 | 95(2) | 18(1) | 61(1) | No data |
| Refused | 3 | 1 | 3 | 3 | 4 | 4 | 8 | 4 | 15 | – | 10 | No Data |

**Box N°8.1: Extradition of Croatian citizens to a non–EU State based on UNTOC Art.16**

In October 2018, pursuant to the Treaty between the US and Serbia from 1901 and United Nations Convention Against Transnational Organised Crime (UNTOC), the US sent a request for provisional arrest for the purpose of extradition of the defendant NN, a citizen of a 3rd country, for numerous offences including drug trafficking, firearms and narcoterrorism offences. He was arrested in October 2018 pursuant to an international arrest warrant issued by Interpol Washington, and the competent judge ordered him an extradition detention. In November 2018, the competent court granted the extradition of NN to the US pursuant to a simplified extradition procedure, and he was extradited to the U.S. in January 2019. In January 2019, pursuant to the Treaty between the US and Serbia from 1901 and UNTOC, the US sent a request for provisional arrest for the purpose of extradition of the defendants JL and JA, who are members of a criminal organisation led by NN. The charges against them relate to their involvement in an illicit transaction involving exchange of drugs for weapons, which NN intended to provide to a terrorist organisation. The competent judge ordered extradition detention. The Court found that statutory preconditions for extradition of JL and JA have been met, and this decision was confirmed by the Supreme Court of Croatia. In September 2019, the MoJA brought a decision granting the extradition of the defendants to the US and they were extradited in October 2019. Given the fact that the SAO of Croatia was also conducting an investigation against JL and JA and that factual description of the offences corresponded to the ones in the US indictment, the competent Court rendered a decision on transfer of criminal proceedings to the US.

794. Similar to the MLA, the international co–operation feedback on extradition was not extensive yet did not identify systematic problems. However, in a few but notable instances, it took more than a year for the authorities to execute some requests. The AT concludes that the lack of a prioritisation mechanism for extradition requests have some impact on the timely execution of the relevant requests.

### *8.2.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements*

795. Croatia seeks MLA to pursue domestic investigations into ML and predicate offences which have a transnational dimension to a limited extent. Given the risk profile of the country and its exposure to broader international threats, this posture might lead the country to miss

[213] Number in brackets are for ML.

opportunities for identifying and investigating relevant cases. The lack of clarification from the country on the low numbers of ML outgoing requests, as well as rejections and the long–term execution of some requests, leads to the conclusion that limited appreciation of ML offence by the Croatian authorities (see IO.7) affects also seeking the MLA and extradition.

*MLA*

796. There is no stable tendency on outgoing requests through the period under consideration. According to the MoJA, through the reporting period, the central authority sent between 500 to 700 requests to foreign judicial authorities. Most of these requests were addressed to jurisdictions within Croatia's close vicinity (including EU and non–EU countries). Croatia issued 89 ML–related outgoing requests (see table 8.8), with an average time for execution of 560 days for ILA and 73 days for EIO, respectively. As for the requests relating to predicate offences (see table 8.9), the timing for execution was around 212 days for ILA and around 123 days for EIO channel. The AT concluded that the long–term execution of specific outgoing requests was attributed to their complex nature (in particular in cases of ML), as well as formal requirements to be met for MLA (i.e., detailed examination of requests for compliance with international instruments, consideration of white copies, translation, etc).

797. The majority of the requests dealing with predicate offences relate to fraud, participation in organised crime, robbery and theft, which refer to the countries risk profile only to some extent. Only a few requests sent deal with the areas of higher threat recognised in the NRA, such as drug trafficking, corruption and tax crimes. This is considered a significant deficiency in Croatia's context. The number of refusals on MLA requests has been the same throughout the whole reporting period, with three dealing with ML. The authorities were not in a position to elaborate on the specific grounds for these refusals. This indicates a lack of proactiveness in analysing the reasons for the refusal in order to improve the quality and timeliness of the requested co–operation.

798. The authorities noted that obstacles might hinder the timely execution of Croatia's MLA requests. Among these: (i) when requested countries do not have "instruments" of simplified judicial co–operation and require communication via competent central authorities or diplomatic channels; and (ii) when dealing with common law countries, the counterparts may take some time to verify the level of proof and usually request additional information. In order to overcome these obstacles, the authorities have initiated the conclusion of specific bilateral agreements on MLA co–operation (see Core Issue 2.1).

**Table 8.7: Outgoing ML requests sent through the SAO**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** | **ILA** | **EIO** |
| Issued | 9 | 2 | 5 | – | 15 | – | – | 4 | 3 | 30 | 13 | 7 |
| Refused | 2 | – | – | – | – | – | – | 1 | – | – | – | – |
| Approx. time | Up to 1060 | 3 and 180 | Up to 421 | – | Up to 910 | – | – | Up to 50 | Up to 289 | Up to 90 | Up to 120 | Up to 60 |

799. As previously indicated, Croatia has increased its use of EIO communication upon the implementation of the EIO Directive. After 2017, the scope of the EIO application was expanded. During the reporting period, EIOs were issued and executed to conduct evidentiary actions, such as obtaining bank information on the account holder and performed transactions, examining

defendants and witnesses, data on subscribers to a certain telephone number/IP address, searches of home and other premises, obtaining documentation, telecommunications contacts and other data. This allowed the authorities to broaden the evidence gathering tools when dealing with criminal offences with an international element.

**Table 8.8: Outgoing requests on predicate offences submitted through SAO**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO | ILA | EIO |
| Issued | 102 | 1 | 74 | 1 | 133 | 10 | 93 | 53 | 53 | 86 | 70 | 113 |
| Granted | 91 | 1 | 67 | – | 120 | 10 | 80 | 43 | 102 | 75 | 60 | 109 |
| Refused | 11 | – | 7 | 1 | 13 | – | 13 | 9 | 11 | 11 | 10 | 4 |
| Average time | 233 | 135 | 221 | N/a | 228 | 130 | 227 | 144 | 223 | 116 | 138 | 90 |

800. During the reporting period, Croatia issued only three freezing orders: one in 2017 relating to a predicate offence and two in 2019 relating to ML. No data was provided for 2020, and the authorities did not elaborate on the outcomes of their requests. No confiscation orders were issued (see IO.8).

801. In addition, Croatia sent nine requests under the Warsaw Convention. The scope of these requests and their output was not provided by the authorities. No other information on the outgoing requests for identification, seizure, confiscation, and repatriation of assets has been provided. On that basis, the AT is of the opinion that the actions taken by the country in this area do not commensurate with its context (see IO.8).

*Extradition*

802. During the whole reporting period, the authorities did not request extradition of the Croatian nationals from non–EU Member States. The co–operation was limited strictly to co–operation within the EU, i.e., through the EAW mechanism. In total, Croatia issued 85 requests (see table 8.9). Throughout the reporting period, there was only one ML–related request in 2017, which was granted. Although in 9 requests, extradition was refused, there was no explanation provided on this matter by Croatia to the AT.

**Table 8.9: Outgoing extradition requests through EAWs**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| Issued | 9 | 4 | 7 | 22 | 22 | 21 |
| Granted | 8 | 4 | 5 | 19 | 19 | 21 |
| Refused | 1 | 0 | 2 | 3 | 3 | 0 |
| Average time | 92 | 91 | 153 | 68 | 71 | 96 |

803. EAWs were promptly recognised and executed – in 95 days on average. Throughout the reporting period, the authorities have increased their efforts of successfully repatriating criminals to its territory via EAW. This demonstrates the proactive approach taken by the authorities in investigating predicate offences with an international element. However, most of these predicates are not linked with higher threats faced by Croatia, as identified in the NRA.

### *8.2.3. Seeking other forms of international co–operation for AML/CFT purposes*

*AMLO*

804. the AMLO actively seeks co–operation on ML/TF cases from the membership through the Egmont Secure Web (ESW) and FIU.net. To further strengthen the co–operation framework with its foreign counterparts, the AMLO has concluded 37 MoUs[214]. In cases where counterparts are not members of any secure network, the AMLO co–operates via alternative means, including crypto messages and fax.

805. The only challenge identified by the Croatian authorities in the context of co–operation with counterparts is the difference in powers and legislation of counterparts that limits the ability of the AMLO to receive the relevant information (such as the holder and turnover of a bank account) in all cases. When these situations arise, the country demonstrates proactiveness by redirecting requests through the LEA direct channels.

806. The average timing for the execution of outgoing requests is within 60 days. In case of potential delays, the AMLO submits the relevant reminders to the foreign FIUs.

**Table 8.10: Outgoing requests sent by the AMLO via ESW**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Outgoing requests | ML | TF | ML | TF | ML | TF | ML | TF | ML | TF | ML | TF |
| Requests sent by the AMLO | 198 | 4 | 106 | 2 | 148 | 0 | 127 | 1 | 105 | 3 | 130 | 0 |
| Spontaneous information sent by the AMLO | 59 | 0 | 96 | 0 | 29 | 0 | 15 | 0 | 18 | 0 | 12 | 0 |

**Table 8.11: Outgoing requests sent by the AMLO via FIU.net**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| Requests sent by the AMLO | 102 | 66 | 88 | 86 | 77 | 66 |
| Spontaneous information sent by the AMLO | 47 | 87 | 26 | 11 | 13 | 7 |

807. Overall, Croatia demonstrated a stable trend in seeking co–operation from its foreign counterparts over the reporting period. There was intense co–operation conducted in 2015, which the AMLO explained to be linked to the analysis of the so–called I–typology. This, however, does not find its confirmation by the written contribution of the AMLO[215], which refers to this typology as being the most intensive in 2018.

808. Most of the requests for information over the observed period were sent to FIUs of Italy, Slovenia, Hungary and Bosnia and Herzegovina, which correlates to the overall geographical exposure of the jurisdiction. Information provided by the country suggests that the majority of outgoing requests are reflecting on ML trends and typologies identified in AMLO's Annual reports, e.g., use of foreign nationals' accounts for ML, VAT and computer frauds. Yet, these do not adequately reflect the findings of the NRA.

809. There has been a clear decrease in spontaneous sharing of information by the AMLO to its foreign counterparts over the reporting period. The authorities explained that the significant

[214] Albania, Armenia, Aruba, Australia, Bahamas, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Czech Republic, Georgia, Guernsey, Indonesia, Israel, Italy, Kazakhstan, Kosovo*, Lebanon, Liechtenstein, Lithuania, Moldova, Montenegro, Netherlands Antilles, North Macedonia, Panama, Paraguay, Poland, Romania, Russian Federation, San Marino, Serbia, Slovenia, Turkey, Ukraine, United Arab Emirates, United States of America.
[215] AMLO Brochure, p.27

number of disseminations at the beginning of the period was linked to a proactive approach of the AMLO to share information linked to the I–typology to one specific counterpart. However, the lack of responsiveness from this counterpart prompted the AMLO to change the approach of communication, by sending information in the form of a request rather than spontaneous dissemination. Nevertheless, this explanation of the change in the trend and the AMLO's approach remains unclear for the AT and raises concern as to what extent the AMLO systematically considers sending spontaneous disseminations to foreign counterparts.

*LEAs*

810. The informal LEA co–operation represents a strong side of the system. This allows to some extent, for overcoming the lengthy MLA processes. The effectiveness of this approach was demonstrated through successful results, including on drug cases (see IO7 and the La Familia case). In order to support domestic investigations, the International Police Co–operation Department within the Criminal Police Directorate performs activities pertaining to international police co–operation within INTERPOL, EUROPOL (SIENA), S.I.Re.N.E. and other international organisations related to international police co–operation. The Police exchanges over 200 000 messages a year. The numbers of ML–related requests are increasing but remain low. Hence, the extent to which the LEAs systematically consider sending spontaneous disseminations to foreign counterparts raises concerns.

811. On a yearly basis, the authorities submit around 100 requests concerning ML, via the Europol channel (SIENA).

**Table 8.12: Number of ML–related SIENA messages sent by Croatian authorities**

| Year | Requests sent |
|---|---|
| 2017 | 22 |
| 2018 | 50 |
| 2019 | 83 |
| 2020 | 89 |

812. Requests mostly feature illegal drugs trafficking along the so–called "Balkan route" and transfer of cash towards Croatia, which is overall consistent with the NRA findings. The Police indicated that they conduct inquires with neighbouring EU and non–EU countries and that the focus is normally on high proceed–generating crimes.

813. Croatia disposes of a regulatory framework for forming joint investigative teams (JITs) with the participation of its counterparts. In practice, it was never used, as the authorities indicated, rather relying on 'JIT–like' informal co–operation to avoid the time–consuming aspects of a formalistic approach. Concerning asset recovery, PNUSKOK is the national contact point for the submission of requests and the exchange of data to trace and identify proceeds of crime. It serves as Asset Recovery Office – ARO. In 2014, Croatia joined the AP Asset Recovery of EUROPOL, connecting its ARO directly to tracing and freezing requests from the EU Member States.

**Table 8.13: Requests sent through the ARO**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests sent | 8 | 7 | 7 | 0 | 5 | 1 | 28 |
| Requests refused | – | – | – | – | – | – | – |

814. Croatia informed that there was no request sent through the CARIN network. The AT was not provided with information on any other platform used by Croatia for tracing, freezing, seizure

and confiscation of proceeds of crime. This highlights a limited approach of the authorities to resort to international co–operation when tracing proceeds of crime abroad.

*Customs Administration*

815. The CA is provided with an adequate legal framework for seeking international co–operation, but no practice was demonstrated. The CA could only elaborate on the use of EU mechanisms, such as the Anti–Fraud Information System (AFIS) portal for searching information on persons and assets to detect cross–border crime and exchange information with counterparts in relation to cash seizures and infringements. The authorities indicated an active use of this tool to get relevant information.

*Tax Administration*

816. In its principal role as a tax authority, the TA seeks co–operation from foreign counterparts including in the framework of EU regulations (mainly in VAT) and double taxation treaties. It can communicate with foreign counterparts, indirectly through the SAO when it exercises its law enforcement powers. The authorities did not provide information that would demonstrate the use of these tools for obtaining ML/TF information.

817. As the designed authority for the supervision of organisers of games of chance, the TA is not provided with an adequate legal framework to communicate and exchange AML/CFT information with its counterparts (see R.40). As the gambling sector is weighted as being important in Croatia based on its materiality and risks, and the online casino activities are growing (see Ch.I), the lack of designated channels or mechanisms for the TA to exchange supervisory AML/CFT information with its foreign counterparts poses a significant concern.

*CNB*

818. As the main financial supervisor in Croatia, the CNB actively exchanges with its foreign counterpart regulatory, prudential and AML/CFT related information. International co–operation is carried out in the framework of membership in various EU platforms, as well as bilateral MoUs.

819. In total, 24 initial requests on AML/CFT matters were sent to 17 foreign authorities over the reporting period, seeking information from foreign supervisory authorities on group supervision. Over the reporting period, very few requests have been sent to foreign countries hosting foreign bank group headquarters. However, these statistics do not reflect that on a routine basis, the CNB exchanges information with foreign counterparts about relevant findings of inspections of subsidiaries and branches performed in their jurisdictions. A recent case was also provided where on–site inspections took place in one country in co–operation with the host supervisor.

820. The CNB also participates in occasional bilateral meetings with other foreign supervisors, including carrying out examinations and subsequent follow–up activities (e.g., with Banca d'Italia in 2020). As of 2021, the CNB is involved in AML/CFT colleges that are set up at the EU level. These aim at achieving effective co–operation and information exchange between prudential and AML/CFT supervisors regardless of the institutional setting of these authorities. Overall, taking into account that the CNB is the licensing and supervising authority for the most important financial sectors in Croatia, many of which are subsidiaries of foreign institutions, the demonstrated active co–operation with its foreign counterparts is commendable.

*CFSSA*

821. Throughout the last few years, the CFSSA focused its communication with foreign counterparts on prudential supervision. The CFSSA demonstrated co–operating with foreign counterparts when conducting market entry fit and proper checks of applicants, including when dealing with multijurisdictional complex structures. According to available statistics, overall, there have been 35 AML/CFT and 7 regulatory requests sent between 2018–2019.

822. The CFSSA is an active member of the International Association of Insurance Supervisors (IAIS), International Organisation of Pension Supervisors (IOPS), International Organisation of Securities Commissions (IOSCO). Participation in these platforms allows the CFSSA to exchange supervisory experience and information when needed.

*Financial Inspectorate*

823. The Financial Inspectorate is the designated authority for supervision of DNFBPs and some types of FIs. These are mostly domestic entities; hence, no practical need has arisen over the past period for the Financial Inspectorate to engage in international co–operation. As described in R.40, the current legal framework regulating the Financial Inspectorate's international co–operation provides with possibility of information exchange with EU Member States, which is relevant for Croatia considering the set–up of its MVTS sector. The AT was informed that Financial Inspectorate has two representatives in the Standing committee for AML/CFT established in 2019 in the European Banking Authority (EBA) framework. They are also a participant in two MVTS colleges. Throughout the reporting period, the Financial Inspectorate has participated in several events aimed at exchanging information, including AML/CFT–related. Potential issues can arise when dealing with non–EU Member States, where the Financial Inspectorate is not provided with an adequate legal framework.

### *8.2.4. Providing other forms of international co–operation for AML/CFT purposes*

*AMLO*

824. Foreign requests are included in the AMLO IT system, allowing for effective case management. When marked as urgent, these requests are dealt with within 4–6 days. However, this does not equate to a formal prioritisation system. So far, there has been no case where the AMLO has refused to provide the requested information nor its consent to disseminate information provided to the foreign FIUs. The top three counterparts submitting requests to the AMLO are Italy, Slovenia and Germany. The AMLO indicated that most of the predicate offences behind suspicious activities were economic crime and tax fraud, which correlates to Croatia's risk profile to some extent only.

**Table 8.14: Incoming requests received by the AMLO via ESW**

| | 2015 | | 2016 | | 2017 | | 2018 | | 2019 | | 2020 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Incoming request** | **ML** | **TF** | **ML** | **TF** | **ML** | **TF** | **ML** | **TF** | **ML** | **TF** | **ML** | **TF** |
| Foreign requests received | 138 | 6 | 107 | 6 | 128 | 5 | 131 | 2 | 113 | 0 | 105 | 2 |
| Foreign requests refused | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Spontaneous information received | – | – | – | – | – | – | – | – | 54 | 2 | 90 | 0 |

**Table 8.15: Incoming requests received by the AMLO via FIU.net**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| Foreign requests received by the AMLO | 127 | 66 | 86 | 94 | 73 | 48 |
| Foreign requests refused by the AMLO | 0 | 0 | 0 | 0 | 0 | 0 |
| Spontaneous information received by the AMLO | – | – | – | – | 41 | 37 |

825. The AMLO indicated that it did not keep records of spontaneous disseminations received from its foreign counterparts before 2019, which explains the missing numbers. The delegations which provided feedback indicated good to excellent co–operation with the AMLO, including swift and valuable replies.

*LEAs*

826. The LEA co–operation is perceived to be timely and of good quality, with isolated cases of non–reply. The co–operation generally correlates to the areas of increased risks. During the observed period, the largest number of requests were received from counterparts in Germany, Italy and the Czech Republic, Hungary, the Netherlands, and Austria. There were no refused foreign requests. Urgent requests are replied to within eight hours. All other requests are handled in a reasonable period, on average, within seven to 14 days.

827. Specific Police departments, such as PNUSKOK and the counter terrorism unit, are directly connected to the EUROPOL channel (SIENA), which enables swift police information exchange.

**Table 8.16: Number of ML–related SIENA messages received since 2017**

| Year | Requests received | Information received |
|---|---|---|
| 2017 | 82 | n/a |
| 2018 | 142 | 30 |
| 2019 | 504 | 69 |
| 2020 | 536 | 30 |

**Box N°8.2. Providing informal co–operation**

On 21.08.2018, the Croatian Police received a request for freezing assets from a law enforcement agency from Country A, following a notification they had received from a bank in their country, whose business partner (a company from Country A) had been a victim of a business email compromise fraud involving false e–mail messages, which they had received from an unknown perpetrator. Namely, on 20.08.2018, the above–mentioned company from Country A transferred USD 136,750.09 to the account of a company in Croatia. Immediately upon the receipt of the notification, the police requested the AMLO to perform activities within its competence. The result was that the payment was not made to the company in Croatia but was returned to the payer on the same day.

The transaction was subject to a criminal investigation conducted by the Police in 2018 and 2019, in coordination with USKOK and in co–operation with the AMLO, against an OCG comprising of Croatian nationals, nationals of Country B and nationals of Country C, connected with financial frauds and ML within a criminal association. The criminal investigation, which involved special investigation techniques and bank transaction analyses, established that one of the suspects, by himself or through other suspects, assumed real management of several companies headquartered in Croatia, in the ownership or under the control of the suspects. After several companies from abroad (from Country A and Country D) had made payments to the accounts of the above–mentioned companies in the amount of at least EUR 3.2 mln. and GBP 680,000 originating from Business Email Compromise (BEC) frauds, most of these financial means were transferred to accounts of companies from Country E, Country F and

Country G, with a part of the funds being transferred to accounts of companies from Country C. They kept the remaining amount for themselves and availed of them to their mutual benefit. In addition to the international police co–operation being achieved through usual channels for the operational exchange of information (Country A, Country G, Country H), meetings were held with foreign LEAs (Country A, Country C, Country G). On the basis of a criminal report, USKOK adopted a decision on the conduct of investigation against six Croatian nationals, one national from Country B and one national from Country C, on reasonable suspicion of their having committed criminal offences and ML within a criminal association.

828. Providing co–operation includes asset recovery through the ARO office, under which Croatia has received an increasing number of requests in recent years. As indicated by the MoI, most requests were sent by the Police, prosecutors and courts from Germany, Italy and the Czech Republic, with normal deadlines for executing requests about seven to 14 days. The requests mainly referred to tracing and identifying proceeds from crime for the purpose of further conducting criminal investigations in relation to fraud, tax evasion and drug abuse committed in the requesting country. No request was refused. Between 2015–2020, various types of assets have been identified (companies, invoices, vessels, vehicles and other property, including real estate with a total value of HRK 57.9 mln. (EUR 7.7 mln.), demonstrating the commitment of Croatia to co–operate effectively with their counterparts.

**Table 8.17: Requests received through the ARO**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests received | 22 | 32 | 58 | 47 | 63 | 61 | 283 |

829. LEAs' foreign counterparts resorted to a lesser extent to CARIN to identify presumably illicit assets. During the observed period, all requests were granted. They mainly referred to tracing and identifying proceeds from crime related to predicate offences of tax evasion, corruption offences and fraud, usually to prepare requests for MLA. This corresponds to the NRA findings to a certain extent only.

**Table 8.18: Number of incoming requests through CARIN**

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | TOTAL |
|---|---|---|---|---|---|---|---|
| Requests received | 6 | 3 | 4 | 7 | 2 | 2 | 24 |

*Customs Administration*

830. The CA disposes of a legal framework for providing international co–operation, but little practice was demonstrated. The CA could only reflect on its efforts made to fill in data to the AFIS portal (no information was provided for 2020), which is used by the EU Member States to search data on persons and circumstances where irregularities are detected. No information was provided on co–operation with counterparts from non–EU Member States.

**Table 8.19: Number of cases entered into CA system (AFIS)**

| Year | Number of cases |
|---|---|
| **2015** | 8 |
| **2016** | 13 |
| **2017** | 10 |
| **2018** | 10 |
| **2019** | 12 |

831. In addition, the CA exchanges risk–related information via the Common Customs Risk Management System of DG TAXUD in the form of Risk Information Forms (RIFs) completed online

and made available instantly to all EU customs offices connected. Over the period 2013–2019, the CA filled eight RIFs. The authorities did not elaborate on their content.

**Box N°8.3: The CA's co–operation under Naples II Convention**

The objective of the Convention of 18 December 1997 on mutual assistance and co–operation between CA (Naples II Convention) is to regulate particular forms of co–operation involving cross–border actions for the prevention, investigation and prosecution of certain infringements of both the national legislation of Member States and Community customs regulations. To that end, EU Member States provide each other with mutual assistance and co–operate with one another through their CAs.

In a request, the customs service of EU country A stated that their competent services were conducting covert investigative measures against a group smuggling large quantities of drugs. The CA was requested to pay special attention when a certain citizen of country B would enter and transit Croatia on a specific date since this person was suspected of hiding a significant amount of cash in a car. According to notification, cash was intended for payment of drugs. In case of detection of cash, the CA was asked to seize the cash and to execute all other legal measures.

The CA (which only had the name and surname of the person) communicated with the MoI. Police officers created a risk profile in the NBMIS (National Border Monitoring Information System) since the system is in their competence. All border crossing points/customs units at the borders and customs competent mobile units were informed about a suspicion of smuggling of cash.

Two citizens of country B arrived at the border crossing point: the EU (Croatia) exit towards country B. CA officers, in co–operation with border police, executed a detailed search of the vehicle, including use of technical equipment – endoscope. No irregularities were found/detected. One person had 6310 EUR in his jacket and the other 710 EUR.

Customs of country A received an answer the same day. The described case did not result in a specific seizure, but it showed how information can be exchanged between two parties in real–time and in a timely manner.

832. Overall, the international co–operation feedback indicated regular exchanges of information, good quality answers with no delays, generally connected to excise violation and budget fraud. There have been very few cases of refusal and failure to provide replies to urgent requests on time.

*CNB*

833. In the course of AML/CFT supervision, the CNB shares findings of its supervisions with the supervisory authority of both parent bank and supervisory authority of the subsidiaries regardless of whether they are in or outside the EU. Since 2014, the CNB regularly shares information with the European Central Bank (ECB) on the risk profiles and supervisory actions towards supervised banks.

*CFSSA*

834. Between 2018–2019, the CFSSA received 19 requests. CFSSA's Regulatory Harmonisation and International Co–operation Division is a central point for receiving such requests. It is responsible for internal coordination and co–operation with the requesting authority. The time

limit for acting on this kind of request is a maximum of 30 days. However, the CFSSA generally responds in a shorter time, especially if the requesting authority requests so.

*Financial Inspectorate*

835. As described above, the international co–operation performed by the Financial Inspectorate is limited to instances of communication with EU Member States. It can provide assistance on a case–by–case basis, as demonstrated below.

**Box N°8.4: International co–operation undertaken by the Financial Inspectorate**

In the context of international co–operation with the supervisory authorities of EU Member States responsible for AML/CFT supervision, and in accordance with national and EU legislation, the FIU of country A, according to the instruction provided by the AMLO, submitted to FI–MoF a request for conducting supervision on the provision of accounting services of company "X", registered in Croatia and company "Y", registered in country A. The FIU A requested information and supporting documentation on whether company X implements CDD measures and whether it reports suspicious transactions in accordance with AML/CFT standards, given that Company Y does not do so in country A.

Following the request, FI–MoF, within its own authority, conducted a supervision on company X and determined that it did not provide accounting services because it has neither technical nor human capacity, but only pre–invoices services, charges, and pays according to invoices from several foreign companies. In May 2019, the FIU A and the AMLO were notified of the supervision findings.

836. Although limited, the overall intentional co–operation feedback identified no issues with respect to the co–operation of financial supervisors.

### *8.2.5. International exchange of basic and beneficial ownership information of legal persons and arrangements*

837. Basic and BO information on legal persons are available in various public registers, such as the court register, the register of associations, register of foundations, as well as the newly established Register of BOs kept by the Croatian Financial Agency – which is still at the stage of being populated. Exchange of BO information is performed by the AMLO, LEAs and supervisors. The country was not in the position to elaborate on the exact statistics for providing the relevant information in the course of international co–operation. However, as described by the authorities, no such request has ever been denied, and the average time for execution has never been more than 30 days. The international co–operation feedback also did not identify any specific issue with such exchange.

838. Nevertheless, limitations observed in IO.5 might impact the provision of accurate BO information by Croatia to its foreign counterparts.

*Overall conclusion on IO.2*

839. Overall, the Croatian authorities demonstrated their ability to provide constructive assistance upon request in the field of MLA, extradition, exchange of information, as well as seizure and confiscation of assets. They co–operate mainly with EU and non–EU neighbouring countries. Nevertheless, the country does not have prioritisation mechanisms in place to deal with incoming requests.

840. More importantly, Croatia does not proactively seek assistance from foreign counterparts and does not co–operate in line with its risk profile. This refers both to obtaining information and tracing proceeds of crime. Despite a significant refusal rate of its outgoing requests, Croatia does not follow up on these in order to identify and eliminate the underlying issues behind it. These two issues have major weighting on the rating.

841. The use of direct and informal channels by competent authorities for providing and seeking information proves to be constructive and timely. While overall, competent authorities disseminate information to their counterparts, the extent to which they systematically consider sharing information spontaneously, raises concerns. The supervisory authorities demonstrated a relatively good level of international co–operation, except for the TA, which is not provided with adequate legal framework and tools to pursue foreign co–operation. The international co–operation feedback did not indicate any specific issue, with exchange of basic and BO information. Limitations observed in IO.5 might impact the provision of accurate BO information by Croatia to its foreign counterparts.

842. **Croatia is rated as having a Substantial level of effectiveness for IO.2.**

## TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to an analysis conducted as part of the previous Mutual Evaluation in 2013. This report is available from https://www.coe.int/en/web/moneyval/jurisdictions/croatia.

### *Recommendation 1 – Assessing risks and applying a risk–based approach*

The requirements on assessment of risk and application of the risk–based approach (RBA) were added to the FATF Standards with the last revision and so were not assessed in the previous mutual evaluation of Croatia.

***Criterion 1.1*** – Croatia completed the first National Risk Assessment (NRA) of money laundering (ML) and terrorist financing (TF) in 2016. In 2018 Croatia initiated an update of the NRA, using the same methodology. The Government adopted the updated report in June 2020. When conducting the NRA Croatia took into account the outcomes of the EU Supra–national risk assessment. NRAs benefited from the input from all key AML/CFT authorities in the country. Nevertheless, the Corruption Prevention Sector of the Ministry of Justice and Administration (MoJA) was not involved in the assessment, and the NRAs did not benefit from their input when considering the level of corruption risk. The private sector participation varied. Major market players took part in person, others through questionnaires, and some sectors were represented by their self–regulatory bodies (SRBs).

Croatia relied on the World Bank tool when assessing the ML/TF risks. Inflexible and inadequate application of certain aspects of the methodology for the 2020 NRA affected findings on the vulnerabilities of the sectors. The assessment of the ML/TF risks in 2020 was impacted by lack of quantitative data and use of diverse information sources when assessing risks (e.g., the main ML threats are identified basing the conclusions on the empirical knowledge of authorities – general expertise and perception of the law enforcement agencies (LEAs). Consequently, this affected the reasonableness of assessment of risks level of certain sectors. The NRA did not assess and did not take into account a number of important vulnerabilities in the system, such as shortage of human resources, etc. (see IO.1)

ML/TF assessment in the NRA is expressed in terms of global ratings for Banking, other FI, DNFBP, Securities and Insurance sectors. Sub–sectors have no specific ML/TF risk assessment but are given vulnerability scores. While the conclusion of the NRA in terms of the relative vulnerability positioning between the sectors (with higher vulnerability sub–sectors of money or value transfer service (MVTS), Games of chance on slot machines, Betting Games (medium high); Lawyers and law firms and then all with equal rating (medium) authorised exchange offices, external accountants and tax advisors) may be appropriate, the level of residual risk attributable to sectors and sub–sectors does not seem reasonable in all cases adversely impacts the ML risk assessment in these sectors.

The banking sector is the most material in Croatia and described in the NRA as the most "commonly misused sector", the two areas of highest vulnerability are consumer transactions accounts (medium high) and non–consumer accounts (high), which aligns with the identified

threats. The Banking sector was considered the relatively highest risk financial services sector, which is supported by the NRA indicating that "a significant number of ML activities begin or at some stage go through the banking sector.

The assessment of the designated non–financial businesses and providers (DNFBPs) suffered from the inflexible use of the tool. Certain sectors were grouped together, and controls were globally assessed in circumstances where there were distinct variations across the different types of DNFBPs. This approach was queried by the sector representatives.

Vulnerabilities in relation to TF are treated identically to ML across each sector, which does not appear to align with the country's context. In addition, where this NRA includes some assessment of TF risk, the information and analysis on which observations and conclusions are based are not clearly identified. Identification and assessment of the TF risks is not sufficient. ML/TF risks in some areas were not appropriately explored (see IO.1).

***Criterion 1.2*** – Responsibility for assessment of national ML/TF risks falls with the Inter–Interinstitutional Working Group for the Prevention of ML/TF (IIWG), (Anti–Money Laundering and Terrorist Financing Law (AMLTFL, Art.5(3)). The IIWG activities and the membership are regulated by the AMLTFL and the Protocol on Co–operation and Establishment of IIWG.

***Criterion 1.3*** – The AMLTFL sets out the legal requirement for Croatia to carry out the NRA every four years or earlier if deemed necessary (Art.5(1)).

***Criterion 1.4*** – The Anti–Money Laundering Office (AMLO) should make results of the NRA available to all reporting entities (REs) and competent authorities, without delay (AMLTFL, Art.6(3)). Both NRAs are published on the website of the Ministry of Finance (MoF)[216].

***Criterion 1.5*** – The AMLTFL sets out the areas for use of the NRA outcomes, this, among others, includes allocation of resources and improving the applied preventative measure (Art. 6(2)).

On the basis of the two NRAs (from 2016 and 2020), Croatia developed the respective Action Plans, which include measures aimed at mitigating the identified ML/TF risks. Both documents include the allocation of resources within relevant authorities and the implementation of other measures to prevent and mitigate ML/TF.

Action Plan from 2016 contains detailed and clear actions aimed at mitigating identified ML/TF risks. Many of the measures, especially in the supervisory field and the area of strengthening implementation of preventative measures, were accomplished. Some actions, such as insufficient capacities of the State Attorney's Office (SAO) and financial investigators, remained unachieved up to now, despite the steps being taken by the authorities. The Tax Administration (TA) of their own volition split their capacity into tax investigations and economic crime/AML investigations to improve their efficiency and performance.

The 2020 Action plan is non–contentious and does not tackle the fundamental issues raised across the two risk assessments, such as lack of successful ML/TF prosecutions, lack of measures regarding detection and confiscation, the need for further training of the judiciary, law enforcement and investigators, inability to secure an adequate number of personnel in the Financial Inspectorate, addressing barriers to recruitment of financial investigators, etc.

[216] https://mfin.gov.hr/istaknute–teme/ured–za–sprjecavanje–pranja–novca/akcijski–plan–za–smanjenje–identificiranih–rizika–od–pranja–novca–i–financiranja–terorizma–u–republici–hrvatskoj/2715

***Criterion 1.6*** – (a) The AMLTFL provides for a limited exemption in relation to electronic money. REs are permitted not to apply certain CDD requirements based on an appropriate risk assessment indicating that the risk is low provided that certain mitigating conditions are met (e.g., limited re–loadability and lack of anonymity) (Art.18). This exemption was directly transposed from the 5th AML Directive without conducting a risk assessment.

There are two types of REs that are not properly designated, and hence the FATF Standards do not apply to them: (i) external accountants for the situations covered under Recommendation (R.) 22 criterion (c.) 1(d) (accountants are not included in AMLTFL, Art. 9(18(1(b)). The sector is assessed as at Medium ML/TF vulnerability; and (ii) VASPs, except for the ones engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers. Assessment of vulnerabilities of the VASPs was conducted recently, concluding that the level of the ML vulnerability is Moderate.

(b) The AMLTFL is not applicable to financial activities if they are conducted on an occasional and limited basis (e.g., accounting for no more than 5% of the turnover in any accounting period, and with a EUR 1 000 threshold for each individual transaction, etc.) (AMLTFL, Art.10). This does not include postal money orders service providers. However, the provisions do not extend to application of these measures on a "very" limited basis (which was explained to be the result of an inflexibility of the Croatian language) and do not exclude other providers of money remittance activities (AMLTFL, Art. 10(1),(3)). It is noted that the Authorised Exchange Offices are rated as Medium risk in the NRA. Croatia advised that there are only 3 REs benefiting from this exception and that the Financial Inspectorate has individually assessed these 3 REs as being at a low level of risk. Croatia has presented statistical data on the turnover of these 3 entities for 2019–2020, which confirm that the size of the business is in line with the AMLTFL. All these proves that the exemption is applied in limited instances. But the exemption is applied not from some requirements under AMLTFL but from all.

***Criterion 1.7*** – The findings of the NRA among others are used to determine the areas of higher ML/TF risks (AMLTFL, Art.6(2)). Croatia meets this criterion through option (a).

(a) REs are obliged to conduct enhanced customer due diligence measures (CDD) to appropriately manage and mitigate ML/TF risks when "high" rather than "higher" ML/TF risk has been established by the NRA. This includes application of enhanced CDD (EDD) when dealing with correspondent relationships, politically exposed persons (PEPs), high–risk jurisdictions, bearer shares, high–risk customers, complex and unusual transactions, or when there is a suspicion of ML (AMLFT Act, Art. 44).

In 2018, in response to risks highlighted in the 2016 NRA, Croatia adopted specific measures to prevent misuse of cash, and mitigate ML threats, such as corruption. These measures are respectively: (i) reducing the CDD threshold for Authorised Exchange Offices and DPMS to HRK 15 000 (EUR 2 000); (ii) requiring that REs collect information on the source of funds when conducting a cash transaction in the amount of HRK 200 000 (EUR 27 000) and more; and (iii) expanding the definition of PEPs to include municipality prefects, mayors, county prefects and their deputies elected on the basis of the Act regulating local elections in Croatia[217]. The 2020 NRA recommends that this threshold be further reduced for authorised exchange offices, which is not included in the 2020 NRA Action Plan.

[217] Reasoning for adoption of the AMLTFL, Ministry of Finance, 2017

(b) REs are obliged to take into account in their risk assessment the outcomes of the NRA (AMLTFL, Art.12(5)).

***Criterion 1.8*** – The findings of the NRA, among others, are used to determine the areas of lower ML/TF risks (AMLFT Law, Art.6(2)). REs may conduct simplified CDD if they have estimated that the customer represents a "low" rather than "lower" ML/TF risk, which is a higher standard than required by the FATF. When deciding such, they must take into consideration the results of the NRA, but not required to ensure consistency with NRA (AMLFT Law, Art. 43 (1–2)). The AMLFT Law sets out measures that may be applied when simplified CDD is considered (Art. 43(3)). The simplified CDD is not allowed when specific higher–risk scenarios apply (AMLFT Law, Art. 43(5)).

***Criterion 1.9*** – The AMLTFL determines the supervisory authority for each category of FI and DNFBP (AMLTFL, Art.81(1)). Supervisory authorities are required to supervise the application of the AMLTFL (Art 82 (1–2), (5–6)). This includes implementing REs' obligations under R.1. Deficiencies, as identified under R.26 and R.28, apply.

***Criterion 1.10*** – REs are required to conduct an assessment of ML/TF risks related to customers, countries or geographic areas, products, services or transactions, and delivery channels (AMLTFL, Art. 12(1)). The risk assessment should be proportionate to the size of RE, type, scope and complexity of its business operations (AMLTFL, Art. 12(3)).

(a) *Document their risk assessments* – REs are obliged to document their risk assessment (AMLTFL, Art. 12(3)). Competent supervisory authorities may determine that individual documented risk assessments are not required for a specific sector of the RE if certain risks characteristic for that sector are clear and understood by that sector (AMLTFL, Art. 12(4)).

(b) *Consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied* – REs are required to consider a broad scope of risk factors. This also includes assessment of the mitigation measures, actions and procedures undertaken by the RE (AMLTFL, Art. 12(2)). Risk analysis should be aligned with Rulebooks, decisions and guidelines of the competent supervisory authorities and take into account the NRA and the Supranational Risk Assessment (AMLTFL, Art. 12(5)).

(c) *Keep assessments up to date* – REs should regularly update their ML/TF risk analysis (AMLTFL, Art. 12(3)).

(d) *Have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs* – REs should submit ML/TF risk analysis to competent supervisory authorities at their request (AMLTFL, Art. 12(3)).

***Criterion 1.11*** – The AMLTFL sets forth the following provisions with regard to risk mitigation measures to be taken by FIs and DNFBPs:

(a) *Have policies, controls and procedures* – REs are required to have written policies, controls and procedures for the mitigation and effective management of ML/TF risks. These should be determined by the REs own risk analysis, including consideration of Rulebooks, decisions and guidelines issued by a competent authority, the NRA and the Supranational Risk Assessment (AMLTFL, Art. 13(1)). Policies, controls and procedures should be adopted by the management of the respective RE (AMLTFL, Art. 13(4)). These should be approved by the management of the RE (AMLTFL, Art. 67(1(1)). The standard nevertheless specifically required this to be done by the senior management, which is deemed to be implied by the reference to the management board.

(b) *Monitor implementation of controls* – REs are required to regularly monitor and review the adequacy and efficiency of the policies, controls, and procedures implemented; and, if necessary, to enhance the measures undertaken by REs (AMLFT Law, Art. 13(4)).

(c) *Take enhanced measures* – Enhanced measures are required to be taken as noted under c.1.7.

***Criterion 1.12*** – Simplified CDD is permitted only where "low" rather than "lower" risk has been identified (AMLFT Act, Art. 43 (1)) (see analysis of c.1.8). REs are prohibited from applying simplified CDD when there is suspicion of ML/TF (AMLTFL, Art. 43(5)). Deficiencies identified in c.1.9 apply.

*Weighting and Conclusion*

Croatia conducted two NRAs to detect its ML/TF risks, but the reasonableness of the assessment casts doubts. Adopted respective Action Plans do not always support application of a risk–based approach to allocating resources and implementing mitigating measures. Limited exceptions are not applied in line with the risks, and when applied, are from all AML/CFT requirements, and the exception of external accountants and VASPs is not supported by the risk assessment. **R.1 is rated PC.**

### *Recommendation 2 – National Co–operation and Coordination*

In the 4th round mutual evaluation report (MER) of 2013, Croatia was rated LC on R.31. The main deficiencies were lack of coordination between AMLO, the Police and prosecutors, resulting in a low number of ML convictions, and lack of coordination with DNFBPs, resulting in low numbers of submitted STRs. Since the last MER, Croatia has implemented various co–operation and co–ordination mechanisms.

***Criterion 2.1*** – There are three strategic documents in Croatia that are aimed at setting policy objectives, in particular, in the area of suppression of corruption and prevention of financing of terrorism. These are respectively the 2015–2020 Anti–Corruption Strategy, the 2015 National Strategy for the Prevention and Suppression of Terrorism and the 2017 National Security Strategy of the Republic of Croatia. These were not, however, driven by the NRA. Among those, only the Anti–Corruption Strategy is revised upon the expiration of the date. No periodicity is set for revision of the other strategies.

In addition to this, Croatia has also adopted two Action Plans developed on the basis of the 2016 and 2020 NRAs, aimed at implementing measures to address identified ML/TF risks. These are described by Croatia as representing the national AML/CFT policy, which raises doubts on the basis of the substance of these: (i) the Action Plans are separate actions prescribed to respective competent authorities, with no overall strategic plan for the IIWG; (ii) it is not apparent how the set actions are linked to and will mitigate the higher ML/TF risks of Croatia.

***Criterion 2.2*** – There is no designated authority or coordination mechanism that holds responsibility for the national AML/CFT policies.

Co–operation and co–ordination on AML/CFT matters are entrusted to the IIWG – an expert working group composed of 11 competent authorities[218] in the field of AML/CFT, coordinated by

[218] The IIWG is comprised of the following competent authorities: Ministry of Justice and Administration, Security Intelligence Agency, State Attorney's Office, Ministry of the Interior, Ministry of Finance (AMLO, Financial Inspectorate, Tax Administration, Customs Administration), Ministry of Foreign and European Affairs, Croatian National Bank, and Croatian Financial Service Supervisory Agency.

the AMLO (AMLTFL, Art.5(3), the Protocol on Co–operation and Establishment of Interinstitutional Working Group for Preventing ML and TF, Art.2). This does not include policymakers – any senior officials, except for the representative of the SAO. Support at the policy–making level is not demonstrated enough for an effective fight against ML and TF. This has also affected successful implementation of some measures set in the 2016 NRA Action Plan.

***Criterion 2.3*** – The IIWG platform – an expert working group serves for co–operation and co–ordination on AML/CFT matters (AMLTFL, Art. 1(23) and 5(5)). Two sub–groups of the IIWG are set to ensure operational co–operation and implementation of national policies in relation to supervisory activities and law enforcement efforts. The AMLTFL (Art.120), provides for a wider range of authorities responsible for the co–operation in preventing and detecting ML/TF than that 11, which are not currently a member of the IIWG. The IIWG does not include policymakers, except for SAO. Operational co–operation is also ensured on the basis of the AMLTFL (Art. 120(1–2), 121–125), Croatian Financial Services Supervisory Agency Law (CFSSA Law) (Art. 15–17) and Memorandum of Understandings (MoUs) signed between the respective authorities (Croatian National Bank (CNB), Croatia Financial Services Supervisory Agency (CFSSA), MoF (including AMLO and Financial Inspectorate).

***Criterion 2.4*** – Croatia has established a Standing Group for the Introduction and Monitoring of the Implementation of International Restrictive Measures (Standing Group) to assist in the co–operation and coordination to combat the PF. The Ministry of Foreign and European Affairs (MFEA) coordinates the activities of the Standing Group (International Restrictive Measures Law (IRM Law) Art. 5(1)). Authorities confirmed that the Standing Group held meetings for the purpose of discussing the amendments to the IRM Law aimed at ensuring compliance of the legislation with the FATF Standards (the law was adopted in 2019).

Croatia also has mechanisms in place to coordinate national efforts in combatting the proliferation of weapons of mass destruction (WMD). The Government has set up a National Commission for the Suppression of WMD Proliferation to ensure implementation of its National Strategy for the Non–Proliferation of WMD adopted in 2013. Authorities also advised that the members of the Standing group are also members of the Commission on the Prevention of WMD. There was no supporting information provided to verify the level and areas of interaction.

***Criterion 2.5*** – Processing of personal data on the basis of and in line with the provisions of AMLTFL is considered as a matter of public interest in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) (AMLTFL, Art. 73(2)). Croatia has co–operation and co–ordination mechanisms in place to ensure AML/CFT requirements comply with data protection and privacy rules. Before adoption, the Croatian Agency for Personal Data Protection gives its opinion to draft AML/CFT legislation on data protection matters (legislation) (Implementation of the General Regulation on Data Protection Law (NN 42/18) – Art.14).

*Weighting and Conclusion*

There are concerns with respect to national AML/CFT policies/strategies, a designated body responsible for co–ordination of national AML/CFT policies and adequacy of mechanisms at policymaking and operational levels. **R. 2 is rated PC.**

### *Recommendation 3 – Money laundering offence*

In the 4th round MER of 2013, Croatia was rated "partially compliant" (PC) on R.1 and "largely compliant" (LC) on R.2. Under R.1, the assessment team identified several technical deficiencies related to criminalisation of ML in accordance with the Vienna and Palermo Conventions and to purposive elements. In addition, several effectiveness deficiencies were identified relating to a low number of ML convictions, no convictions for autonomous ML and lack of opportunity to access the effectiveness of the new Criminal Code (CC). Since then, Croatia has taken steps to address the majority of deficiencies identified in the 4th round MER. Since then, the Parliament of Croatia adopted the "Act on Amendments to the Criminal Code" on 14 December 2018 (Official Gazette No. 118/18). Some minor deficiencies remained, e.g., the person who commits the predicate offence could not be the perpetrator of the ML offence committed through acquisition, possession or use of the proceeds of crime; the subject matter of the ML offence, as defined by the new CC, does not cover all types of property; shortcomings in the definition of TF as a predicate offence.

***Criterion 3.1*** – ML is criminalised under the CC (Art. 265). The ML offence broadly incorporates the elements of the Palermo Convention (Art.6(1)) and Vienna Convention (Art.3(1)(b)&(c)). Investing, taking over, converting, transferring, and replacing proceeds of a criminal offence to conceal or disguise its illegal origin and concealing or falsely presenting the true nature, origin, place, disposition, transfer and existence of the right, i.e., ownership of the proceeds of crime are all defined under the ML offence. It is a crime to commit ML both by intent and negligence.

***Criterion 3.2*** – CC (Art.265) criminalises the laundering of proceeds from "criminal offence", which means any offence defined as an offence by the CC. Therefore, Croatia has an all–crimes approach. Nevertheless, there remain some gaps in criminalisation of TF, impacting the range of offences that should be covered.

***Criterion 3.3*** – This criterion is not applicable because Croatia applies an all–crimes approach.

***Criterion 3.4*** – The corpus delicti of ML is the "proceeds derived from criminal offence". "Pecuniary advantage" is defined under CC (Art.87(22)), as "[…] a direct pecuniary advantage obtained by the commission of the criminal offence, the property into which the direct pecuniary advantage obtained by a criminal offence has been changed or converted to, as well as any other benefit obtained from the direct pecuniary advantage obtained by a criminal offence or property into which the direct pecuniary advantage obtained by a criminal offence has been changed or converted to […]". The CC (Art. 87(23)) defines property as follows: "property of any type is considered to be the property, regardless of if the property is tangible or intangible, moveable or immoveable, i.e., legal documents or instruments which serve as proof to the right to the interest in such property or of an interest in such property".

Although the ML offence extends to "*proceeds of crime*", the definition of "*proceeds of crime*" and "*property*" seems broad enough to cumulatively cover the scope in relation to the FATF Standards.

***Criterion 3.5*** – No legal requirement does exist requiring a prior conviction for the predicate offence to convict for ML.

***Criterion 3.6*** – Predicate offences for ML committed outside of Croatia extend to conduct that occurred in another country which constitutes an offence in both the foreign country and Croatia (CC, Art. 265(7)).

***Criterion 3.7*** – Self–laundering is criminalised in all cases, except for acquisition, possession, and use of proceeds of crime. Croatian authorities state that criminalisation of self–laundering is contrary to Constitutional principle but indicate no exact provision that would justify this. The Supreme Court in its jurisprudence (I Kž 625/13–6 28.05.2015 and I Kž 560/16–4 08.09.2016) did not highlight any constitutional obstacle for self–laundering, rather stated that placement of money obtained by commission of the predicate offence in the bank accounts and latter withdrawal of cash do not represent ML offence. The assessment team, therefore, found no legal obstacle to criminalise self–laundering.

***Criterion 3.8*** – It is possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances. Although the CC does not explicitly state this, the Criminal Procedure Code (CPC) (Art.450) establishes that the court is bound to conscientiously assess each piece of evidence individually and in relation to other evidence and based on such assessment to reach a conclusion on whether or not a particular fact has been proven and, therefore, the rule of the free assessment of evidence applies.

***Criterion 3.9*** – The general sanction regime applicable to natural persons for committing ML is proportionate but not fully dissuasive. The applicable sanction for ML (CC, Art.265(1)) is imprisonment of a maximum of five years. For high–value ML (involving laundering of proceeds of high value), it is up to eight years imprisonment (CC, Art.265(5)). Negligent ML is punishable with up to three years imprisonment (CC, Art.265(6)). In addition, imprisonment penalties for ML offences can be suspended (CPC, Art.56). Furthermore, for ML, the financial penalties are not compulsorily. Comparing sanctions' range for ML with other serious criminal offences (such as drug trafficking and trafficking in human beings) it is evident that envisaged sanctions are not fully dissuasive. Those deficiencies are minor.

***Criterion 3.10*** – Legal persons are criminally liable for ML, with the act of ML defined on the same basis as an act committed by a natural person. The responsibility of legal persons is based on the guilt of the responsible person, and the legal person shall be punished for the criminal offence of the responsible person also in cases when the existence of legal or actual obstacles for establishing responsibility of responsible person are determined.

Sanctions are prescribed by the Responsibility of Legal Persons Law (RLP Law) and are proportionate but not dissuasive. Namely, a legal person convicted of an ML offence is subject to fines up to HKR 10 mln. (EUR 1.3 mln.) (RLP Law, Art.10(2)), or in case of aggravated ML up to HKR 12 mln.(EUR 1.6 mln.) (RLP Law, Art.10(3)). A legal person may be permanently terminated only if the legal person was founded for the purpose of committing criminal offences or mainly used its operations for committing criminal offences (RLP Law, Art.12(1)).

***Criterion 3.11*** – The ancillary offences to ML offence include: participation in, association with, or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission of an act of ML (CC, Art.34, 36(2), 37–38).

*Weighting and Conclusion*

Croatia is in line with the most of requirements under R.3. Minor deficiencies are identified with respect to: the range of criminalised predicate offences as described under R.5, criminalisation of self–laundering, dissuasiveness of sanctions applied to natural persons and legal persons**. R.3 is rated LC.**

## Recommendation 4 – Confiscation and provisional measures

In the 4th round MER of 2013, Croatia was rated PC on R.3 due to, amongst others, the definition of "pecuniary advantage" did not fully comply with the standards, the confiscation of property of a corresponding value of the instrumentalities was not explicitly covering incorporeal assets and the regulations related to provisional measures were heterogeneous. Since then, Croatia has taken steps to address the majority of deficiencies identified in the 4th round MER. Some minor deficiencies remained, e.g., the definition of the pecuniary advantage, as the subject matter of confiscation, provided by the new CC, does not explicitly cover incorporeal assets and legal documents or instruments evidencing title to, or interest in such assets; the confiscation of property of a corresponding value of the instrumentalities is not provided; CPC (Art.261) was limited to "objects which have to be seized pursuant to the CC", and it is unclear if the scope of "objects" entirely extended over the scope of "funds".

***Criterion 4.1*** – Croatia applies a conviction–based confiscation regime, as well as some form of non–conviction–based confiscation (CPC, Art.560–560.f). CC and CPC provide the confiscation of the following:

(a) *Property laundered* – Confiscation of property laundered by persons convicted for ML is mandatory (CC, Art. 265 (9)).

(b) *Proceeds of (…), or instrumentalities used or intended for use in, ML or predicate offences* – In Croatia, no person shall retain the property gained through unlawful act (CC Art. 5). Proceeds of crime shall be confiscated on the basis of a court decision establishing the commission of an unlawful act (CC, Art. 77(1)). Confiscation of proceeds of crime is mandatory even from the person to whom it is transferred if it is not acquired in good faith. The definition of proceeds is sufficiently broad to encompass benefits *derived from* proceeds of ML or predicate offences (CC, Art. 87(22)). Instrumentalities and objects used for the commission of the criminal offence shall also be confiscated (CC, Art. 79(1)). Confiscation of instrumentalities and objects that were intended or used for the commission of a criminal offence is mandatory for ML (CC, Art. 265(9)), but not for all predicate offences (CC, Art.79(2)).

(c) *Property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations* – Property that is proceeds of terrorism, financing of terrorism or terrorist organisation would qualify as proceeds of crime gained from commission of a criminal offence and shall be confiscated (CC, Art.77). Confiscation is required for funds collected or provided directly or indirectly with the aim of using them or knowing that they will be used, in whole or in part, for the purpose of committing or contributing to the commission of certain types of terrorism–related criminal activities as defined in the CC, or by a terrorist or terrorist association (CC, Art. 98(3)). However, the term "funds" is not defined, and it causes doubts whether the requirement does extend to any type of property.

(d) *Property of corresponding value* – In cases where confiscation of "*objects and rights acquired as pecuniary advantage*" is impossible, the perpetrator shall pay *"the corresponding money equivalent*". Other property can be targeted in the execution stage of the conviction. There are no such provisions relating to confiscation of a corresponding value of instrumentalities used or intended for use in the commission of ML, TF or other predicate offence (CC, Art.77(4)).

***Criterion 4.2*** – (a) *identify, trace and evaluate property that is subject to confiscation* – Croatia has measures that enable its competent authorities to identify, trace and evaluate property that is subject to confiscation.

Proceeds gained through the commission of the criminal offence shall be investigated by prosecutor *ex officio*. SAO shall undertake necessary measures to establish the value of the pecuniary advantage and the location of the unlawfully obtained property (CPC, Art. 206i). In case of tracing high–value proceeds of crime from the offences that are within the competences of the County Court, financial investigators can be engaged to conduct joint investigations.

In this regard, SAO is entitled to request data from state authorities and legal entities except those representing secrecy (which can hinder identification or tracing of proceeds (see. C.4.2(b)). SAO is not empowered to compulsorily and directly obtain data that constitutes banking secrecy but can do so following a Court order (CPC, Art.265).

SAO can request banking entities and other bodies (i) to check the business dealings of a legal or natural person; (ii) to temporarily seize money, securities, items and documents that can serve as evidence; (iii) to monitor and provide information which can serve as evidence of the committed criminal offence or of the proceeds of crime, and (iv) may also request information on collected, processed, and stored data related to unusual and suspicious monetary transactions (CC, Art.206g).

Office for the Suppression of Corruption and Organised Crime (USKOK) can request the bank to submit information on accounts in case USKOK has information that a certain person receives, holds, or otherwise operates through his bank accounts with the proceeds of a particular criminal offence but, if the banking institution does not do so, a Court order is needed to obtain this information.

Police are entitled to collect data on proceeds of crime (Police Duties and Powers Law (PDPL), Art.23). Police duties are performed *ex officio* or based on the request of the SAO (PDPL, Art.4, CPC, 206(4)). Furthermore, the Police are authorised to undertake a preliminary investigation and inform the SAO of the outcomes of its actions (CPC, Art.207).

(b) *carry out provisional measures, such as freezing or seizing, to prevent any dealing, transfer or disposal of property subject to confiscation* – temporary seizure of objects is prescribed under the CPC (Chapter XVIII, Part 2) and is done without prior notice to the holder of the property (CPC, Art.557b (2)). However, temporary seizure orders would not apply to files and other documents of state authorities the publication of which would violate the confidentiality obligation (e.g., it could hamper corruption investigations) or tapes and private diaries found with the persons exempted of the duty to testify (this exemption is not applicable to some crimes, but applicable to ML and TF and a large number of predicate offences). Provisional measures, such as the prohibition of disposal of real estate, the "seizure and depositing of cash and securities or the prohibition to a bank to pay out an account to the defendant or another person to whom proceeds have been transferred, can be ordered to ensure the confiscation (CPC, Art.557a).

(c) *take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation* – Court is entitled to confiscate proceeds of crime from the person to whom it is transferred if it is not done in good faith (CC, Art.77(1)).

(d) *take any appropriate investigative measures* – Investigative measures are provided by the CPC and other relevant legal acts. Deficiencies under R.31 apply.

***Criterion 4.3*** – Bona fide third parties' property is exempted from confiscation (CC, Art.77(1)). These parties may challenge the provisional measures order through the appeal procedure (CPC, Art.557a). Furthermore, the third–party whose property may be affected by a possible confiscation shall be informed of the judicial proceedings and is entitled to take part in the trial

in order to exercise its right of defence through the same means used by the suspected, accused, or convicted person (CPC, Art. 558). The third–party also has the right to appeal against the court decision by which confiscation of the instrumentalities or proceeds is ordered (CPC, Art.464(5)).

***Criterion 4.4*** – Ministry of Physical Planning, Construction and State Assets (MPPCSA) is responsible for management of temporary seized property, including instrumentalities used or intended to be used in the commission of the criminal offence (State Property Management Law Art.59). This management includes the possibility to sell this property if the storage is dangerous, if its cost is disproportionate to the value of the seized property, or if an imminent danger of deterioration/significant loss of value exists. The seized property could also be leased or rented. Once the property is confiscated, it becomes state property. In such case, property is managed in the same manner as other state property. Regarding the management of seized property, Croatia has a separate Regulation on the conditions and methods of management of the temporarily seized property in criminal proceedings: movable, immovable, shares, money, securities, etc. However, there is no legal provision enabling management of the seized legal persons.

*Weighting and Conclusion*

Croatia meets most of the criteria under R.4. Deficiencies identified are the lack of mandatory confiscation of instrumentalities intended for the use in the commission of the majority of predicate offences. In addition, confiscation of corresponding value for instrumentalities is not regulated. There is no definition of "funds" in the CC. There are some unreasonable restrictions in relation to the seizure of objects related to the offence and relevant for investigation. Management of the seized legal persons is not regulated. Deficiencies under R.31 have bearing on the rating. **R.4 is rated LC.**

## Recommendation 5 – Terrorist financing offence

In the 4th round MER of 2013, Croatia was rated LC on SRII. The scope of the term "terrorist" and "terrorist organisation", derived from logical and systemic interpretation of different articles of the CC, were narrower than envisaged by the FATF standards. Since then, Croatia has taken steps to address some of the deficiencies identified in the 4th round MER.

***Criterion 5.1*** – Croatia criminalises TF offence (CC, Art.98) as providing or collecting of funds, directly or indirectly, with the intention that they be used or in the knowledge that they will be used, in full or in part, to carry out the following crimes: terrorism (CC, Art.97), public incitement to terrorism (CC, Art.99), recruitment for terrorism (CC, Art.100), training for terrorism (CC, Art.101), travelling for the purpose of terrorism (CC, Art.101.a), terrorism association (CC, Art.102), preparing criminal offences against values protected under international law (CC, Art.103), kidnapping (CC, Art.137), destruction of or damage to public–use devices (CC, Art.216), misuse of radioactive substances (CC, Art.219), attack on an aircraft, vessel or immovable platform (CC, Art.223), endangering traffic by dangerous act or means (CC, Art.224), murder of an internationally protected person (CC, Art.352), kidnapping of an internationally protected person (CC, Art.353), attack on an internationally protected person (CC, Art.354), threat to an internationally protected person (CC, Art.355), or another criminal offence aimed at cause the death or serious bodily injury of a civilian or other person not actively involved in an armed conflict, if the purpose of the act is to intimidate the population or force a state or international organisation to do or not do something.

The acts which constitute an offence within the scope of and as defined in the 1997 International Convention for the Suppression of Terrorist Bombings are covered to some extent under the

criminal offence of terrorism (CC, Art.97). However, placing and discharging an explosive or other lethal device as defined in this Convention is not covered. Therefore, financing of this activity is not criminalised.

Croatia did not ratify the 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.

***Criterion 5.2*** – According to CC (Art.98(1–2)), financing of terrorism refers to providing or collecting funds, directly or indirectly, with the intention of using them in whole or in part, in Croatia or abroad: (i) by a terrorist association (organisation) or a terrorist or (ii) to commit one or more terrorist acts or other criminal offences, such as the misuse of radioactive substances. A link to a specific terrorist act or acts is not required by the CC. The term "terrorist association" is defined by CC (Art.102 "Terrorist association"), which refers to the persons who organise or direct others to commit terrorist acts and to those who commit an act with the knowledge that such act contributes to the achievement of the terrorist association's goal. Although funds were defined in 2019 by the AMLTFL, it was only done "in the context of [AMLTF] Law", funds and other assets are not defined in the context of the CC and, therefore, it is not evident that it can be used for the purposes of criminal investigation of TF offence.

***Criterion 5.2bis*** – CC (Art.98) criminalises, amongst others, financing the criminal offence established at CC (Art.101.a, and 103). This Article criminalises travelling for the purpose of the commission or contribution (i.e., solicitation, aiding and abetting) to the commission of terrorist acts, the providing or receiving of terrorist training or to take part in a terrorist association. The above provisions do not expressly state that such travels include the perpetrators' travel to "another State other than their States of residence". However, nothing in the provision's wording suggests that such travels are limited to the territory of the States of the perpetrators' residence. CC (Art.101) covers most of the elements for provision of training but is limited to special techniques and methods only. While financing of travel for the purposes of participation in a terrorist act is criminalised, financing of travel for the purpose of preparation of a terrorist act may not be considered as a criminal offence.

***Criterion 5.3*** – The wording "funds" in the TF offence (CC, Art.98) does not specify a source, so it can be concluded that it refers to any funds, whether from a legitimate or illegitimate source. The term "funds" is defined in the context of AMLCFT Law (stating for the purpose of this law) and is not defined in the context of the CC. Therefore, it is not evident whether, in terms of criminal offence of financing of terrorism, it covers all funds and other assets as defined in the FATF Standards.

***Criterion 5.4*** – Croatia does not require that funds be actually used in order to perform or attempt a terrorist act or that they should be linked to a specific act (CC, Art.98). TF offence only requires "the intention" that the funds should be used for terrorist purposes, including as autonomous conduct its use by a terrorist or terrorist organisations, even in the absence of a link with a specific terrorist act.

***Criterion 5.5*** – Although the CC does not explicitly state that in case of TF, proof of intention can be adduced from objective factual circumstance, CPC (Art. 450) establishes that the court is bound to conscientiously assess each piece of evidence individually and in relation to other evidence and on the basis of such assessment to reach a conclusion in whether or not a particular fact has been proved and, therefore, the rule of the free assessment of evidence applies. Consequently, it is possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances.

***Criterion 5.6*** – Persons convicted for TF may be sentenced to a prison term between 1 and 10 years (CC, Art.98). There is flexibility for judges to reduce minimum sentences based on especially mitigating circumstances to 6 months. These sentencings appear to be proportionate to other terrorism–related crimes since the same punishment can be applied for public incitement to terrorism (CC, Art.99), recruitment for terrorism (CC, Art.100), providing training for terrorism (CC, Art.101(1)). These sanctions are proportionate and dissuasive.

***Criterion 5.7*** – Criminal liability of a legal person is founded on the guilt of a responsible natural person. The liability of a legal person shall not prevent the liability of a natural person. Criminal proceedings against the legal person can be launched even if no criminal proceeding may be instituted or concluded against the responsible natural person (RLP Law, Art.23). Sanctions are prescribed by the RLP Law. These are proportionate but not dissuasive. Namely, legal persons convicted for TF offence are subject to fines up to HKR 12 mln. (EUR 1.6mln.) (RLP Law, Art.10(3)) and the termination of the legal person (RLP Law, Art.12(1)). However, a legal person may be permanently terminated only if the legal person was founded for the purpose of committing criminal offences or mainly used its operations for committing criminal offences.

***Criterion 5.8*** – The ancillary offences are fully covered in CC:

*(a) Attempt to committee TF offence* – is covered through CC, Art.34 (attempt).

*(b) Participating as compliance in a TF offence or attempted offence* – is covered through CC, Art. 36(2) (co–perpetration).

(c) *Organising or directing others to commit a TF offence or attempted offence* – is covered through CC, Art. 37 (abetting). Croatia also has separate criminal offences for public incitement to terrorism (CC, Art.99) and terrorist association (CC, Art.102).

*(d) Contribute to the commission of one or more TF offence(s)*...– is covered through CC, Art. 102(2).

***Criterion 5.9*** – Due to the all–crimes approach applied in Croatia, the TF offence is a predicate offence for ML.

***Criterion 5.10*** – Croatian CC does not make any distinctions regarding the place where the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur. If the terrorist(s)/terrorist organisation(s) is located in another country or the terrorist act(s) occurred/will occur in another country and the person alleged to have committed the financing of these persons or these acts is in Croatia the terrorist financing offence appears to be applicable. There does not appear to be anything in the legislation which limits the TF offences in contravention of this criterion. Furthermore, CC (Art.16) establishes that Croatian criminal legislation applies to anyone outside the Croatian territory who commits a terrorism offence (CC, Art.97).

### *Weighting and Conclusion*

Most of the criteria under R.5 are met by Croatia. However, financing the offences from the 1997 International Convention for the Suppression of the Terrorist Bombing are not fully covered. The term "funds and other assets" is not defined in the context of the CC. Financing of travel for the purpose of preparation of a terrorist act is not considered as a criminal offence. Sanctions applicable for legal persons are not dissuasive. **R.5 is rated LC.**

### *Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing*

In the 4th round MER of 2013, Croatia was rated PC on SR.III. The summary of the factors underlying this rating were: concerns over the concept of "assets"; the narrower scope of assets and other property subject to freezing; no effective mechanism in place to designate persons in the context of UNSCR 1373(2001); concerns over freezing without prior notification taking in place only at the level of guidelines; no sanction in place for freezing assets with prior notice to the designated persons; lack of legal procedure to examine and give effect to the actions initiated under the freezing mechanism of other jurisdictions; no procedure for communication of the consolidated lists to REs; and effectiveness–concerns related to the general lack of understanding by the REs about the mechanism of freezing of funds used for TF.

Since the adoption of the MER, Croatia adopted the "Law on amendments to the Law on International Restrictive Measures" on 14 June 2019, which is the main national legislative instrument through which UN and EU sanctions are implemented. This has been done in order to enhance compliance with R.6. In addition, following accession to the EU on 1 July 2013, Croatia applies the freezing mechanisms through EU legislation.

Croatia implements UNSCR 1267/1988 (on Afghanistan) through EU Regulation 753/2011 and Council Decision 2011/486/CFSP, and UNSCR 1267/1989 (on Al Qaida) through EU Regulation 881/2002 (and its successors) and Common Position 2002/402/CFSP. These Regulations have direct legal effect in Croatia. Neither EU nor domestic legislation does deal with EU internals.

In July 2019, the MONEYVAL plenary adopted the exit follow–up report submitted by Croatia. It has concluded that while some steps are done by the authorities, there are still important gaps in the system.

***Criterion 6.1*** – In relation to designations pursuant to UNSCR 1267/1989 and 1988:

(a) The authority responsible for introduction, monitoring and coordination of the implementation of the restrictive measures in Croatia is the Standing Group. There is no explicit provision, however, defining the power of the Standing Group to propose persons or entities for designation to 1267/1989 and 1988 UN Committees.

(b) There is no formal procedure in place establishing the process for detection and identification of targets for designation based on the designation criteria set out in the UNSCRs.

(c) Apart from the general term "evidentiary standard" used in the criminal proceedings, there are no specific rules on the evidentiary standard when deciding whether or not to make a proposal for designation.

(d) There are no procedures in place with respect to filing information with UN Sanctions Regimes in support of proposed designations. Alternatively, no examples of the use of such forms have been provided.

(e) There is no requirement to include a wide range of information on the targeted individual or entity as part of the proposal to allow for accurate and positive identification, as well as including a detailed statement of the case in support of the proposed listing. No provision exists indicating whether Croatia may be made known to be the designating state. Alternatively, no examples to demonstrate the practice have been provided.

***Criterion 6.2*** – In relation to designations pursuant to UNSCR 1373:

(a) *At the EU level*, the EU Council is the competent authority for making designations according to EU Regulation 2580/2001 and EU Council Common Position 2001/931/CFSP. This does not include persons, groups and entities having their roots, main activities and objectives with the EU (EU internals). Domestic legislation does not deal with EU internals.

*At the national level and upon request from another country,* pursuant to IRM Law (Art.5(2)), the Standing Group is authorised to propose to the Government of Croatia to introduce restrictive measures with regards to specific natural, and legal persons and other entities upon its members own initiative, or at the proposal of another country. Based on these proposals, the Government may only propose to the EU Council to issue a relevant decision on international restrictive measures according to IRM Law (Art.5(3)(4)). There is no explicit provision defining the power of the Government to make a designation pursuant to UNSCR 1373.

(b) *At the EU level,* the Common Position 2001/931/CFSP on the application of specific measures to combat terrorism Group ("COMET Working Party") of the EU Council applies designation criteria consistent with the ones in UNSCR 1373.

*At the national level,* there is no mechanism for identifying targets for designation based on the designation criteria set out in UNSCR 1373.

(c) *At the EU level,* requests for designations are received and examined by the COMET Working Party, which evaluates and verifies the information, including the reasonable basis for the request, to determine whether it meets the criteria set forth in UNSCR 1373.

*At the national level*, no formal procedure in place ensuring the verification for prompt determination of designation requests received from non–EU Member States.

(d) *At the EU level*, The COMET Working Party assesses whether the request is substantiated enough and meets the designation criteria stipulated under Common Position 2001/931/CFSP. It further makes a decision on the recommendation to be adopted by the EU Council, based on reliable and credible evidence, without it being conditional on the existence of an investigation or conviction. No clear time limit has been set for the Working Party's review.

*At the national level*, apart from the general term "evidentiary standard" used in the criminal proceedings, there are no specific rules on the evidentiary standard when deciding whether or not to make a designation.

(e) *At EU the level,* there is no specific mechanism that would allow for requesting non–EU Member States to implement the EU restrictive measures.

*At the national level*, there is no formalised procedure under which Croatia could ask another country to give effect to freezing measures undertaken by Croatian authorities.

***Criterion 6.3*** - (a) *At the EU* level, all EU Member States are required to provide each other with the widest possible range of police and judicial assistance on TFS matters, inform each other of any actions taken, co–operate and supply information to the relevant UNSCs (EU Regulation 881/2002 (Art.8); EU Regulation 2580/2001(Art.8); CP 2001/931/CFSP (Art.4)).

*At the national level*, Croatia has not provided information that would deal with collecting information in order to identify a person meeting the designation criteria.

(b) *At the EU level*, as for the UNSCRs 1267/1989 and 1988 regime, EU Regulation 1286/2009 provides for *ex parte* proceedings against a person or entity whose designation is considered. The

Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the designation.

*At the national level*, there is no explicit provision for operation *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered.

***Criterion 6.4*** – *At the EU level*, implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not yet occur "without delay." An expedited procedure has been adopted by the Commission for implementation of new listings required by for UNSCR 1989 transposed under EU Regulation 881/2002. The delay between the date of designation by the UN and the date of its transposition into the EU framework has consequently shortened but is still not consistent with the requirement to implement sanctions "without delay". For resolution 1373, TFS are implemented without delay because, once the decision to freeze has been taken, EU Regulation 2580/2001 is immediately applicable within all EU Member States.

*At the national level*, there is no explicit provision related to the implementation of TFS "without" delay.

***Criterion 6.5*** – The IRM Law (Art.5(1)) establishes the Standing Group headed by the MFEA as a responsible authority for monitoring and coordinating the implementation of restrictive measures under the IRM Law.

(a) In relation to UNSCRs 1988 and 1267/1989, EU Regulations establish the obligation to freeze all the funds and economic resources belonging to a person or entity designated on the European list: EU Regulation 881/2002 (Art.2(1)), as amended by EU Regulation 363/2016 and EU Regulation 753/2011 (Art.3).

For UNSCR 1373, the obligation for natural and legal persons to freeze the assets of designated persons derives automatically from the entry into force of the EU Regulation, without any delay and without notice to the designated individuals and entities (EU Regulation 2580/2001 (Art.2(1a)). Listed EU "internals" are not subject to freezing measures but only to increased police and judicial co–operation among members (CP 2001/931/CFSP footnote 1 of Annex 1).

The IRM Law (Art.11(a)) obliges natural and legal persons and other entities to freeze the assets and other property. The assets and other property of entities against whom the restricted measures are implemented shall be frozen without prior notification/announcement to the entities according to the IRM Law (Art.11(1(d)). According to Item 2 of the Government decision on the manner of implementing international measures to restrict the disposal of property (OG 1651/2011), all assets defined under the IRM Law (Art.3) shall be frozen without delay. However, this does not extend to freezing of assets of EU "internals".

(b) Pursuant to UNSCR 1267/1989 and 1988, the freezing obligation extends to all funds and other assets that belong to, are owned, held or controlled by a designated person or entity. The obligation to freeze the funds or assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities is covered by the notion of "control'' in the EU Regulations 881/2002 and 753/2011. However, with regard to UNSCR 1373, under EU Regulation 2580/2001 the freezing obligation does not cover the funds or other assets which are jointly owned or controlled and a sufficiently broad range of assets under the EU framework –.

Pursuant to IRM Law (Art.11), the freezing actions refer to "freezing all the assets and other property owned, held or belonging in any other way to the entity against whom the measures are applied, or which are controlled or supervised by that entity, and the assets and other property under the joint or indirect control of the entity". The IRM Law includes the '' jointly owned or

controlled assets''. However, the requirement to freeze the funds and assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities and the funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities, is not covered under the IRM Law.

(c) In compliance with the UNSCRs, EU Regulations 881/2002 (Art.2(2)), 753/2011 (Art.3) and 2580/2001 (Art.2(1–2)) prohibit EU nationals and all other persons or entities present in the EU from making funds or other economic resources available to designated persons or entities.

The IRM Law (Art. (11(1(b)) prohibits making the assets available, directly or indirectly, to the entity against which the measures are applied, and persons acting on behalf of or for the account of the entity may not control or have them in their possession. However, some elements, such as wholly or jointly, for the benefit of designated persons, entities owned or controlled, directly or indirectly by designated persons, are not covered under the IRM Law. In addition, ''financial or other related services' to be prohibited from making available to those designated, are not covered. No requirement that ''country should prohibit [...] unless licensed, authorised or otherwise notified in accordance with the relevant UNSCRs'' is set.

(d) *At EU level,* EU Regulations, including designations decided at the European level are published in the *Official Journal* of the EU and website and included in a consolidated financial sanctions database maintained by the European Commission, with an RSS feed. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures.

*At national level*, according to the IRM Law (Art.5–7), the government shall establish a Database of implemented restrictive measures, which is accessible to the natural and legal persons and other entities to whom it refers. The list of natural and legal persons and other entities subject to EU and UN restrictive measures are available on the website of the MFEA pursuant to the IRM Law (Art.10(4)). There is no mechanism for active communication of designations to FIs and DNFBPs. No guidance is provided to REs on their obligation in taking actions under the freezing mechanism.

*(e) At EU level,* natural and legal persons (including FIs/DNFBPs) are required to provide immediately any information about accounts and amounts frozen under EU legislation according to EU Regulation 881/2002 (Art.5.1), EU Regulation 2580/2001 (Art.4), and EU Regulation 753/2011 (Art.8).

*At national level*, there is a general requirement to notify the MFEA on the application of restrictive measures (IRM Law, Art.10(1)). No requirements are in place for reporting attempted transactions.

*(f) At EU level,* EU Regulations protect third parties acting in good faith (EU Regulations 881/2002 (Art.6); and 753/2011(Art.7)).

*At national level*, there is no specific rule for the protection of *bona fide* third parties acting in good faith when implementing the obligation under UNSCRs.

***Criterion 6.6*** – Croatia does not have publicly known procedures for de–listing. The general regulatory framework on un–freezing of assets is set in the IRM Law.

(a) At EU level, there are procedures to seek de–listing through EU Regulations (EU Regulation 753/2011 (Art.11(4)) for designations under UNSCR 1988, and EU Regulation 881/2002 (Art.7a and 7(b(1)) for UNSCR 1267/1989).

*At national level*, there is no specific procedure for submitting de–listing requests to the relevant UN Sanctions Committee.

(b) *At EU level*, for 1373 designations, the EU has de–listing procedures under EU Regulation 2580/2001. De–listing is immediately effective and may occur ad hoc or after mandatory 6–monthly reviews.

*At national level*, there are no procedures in place.

(c) *At EU level*, designated persons or entities affected may write to the Council to have the designation reviewed or institute proceedings according to Treaty on the Functioning of the European Union (Art. 263(4) and 275(2)) before the EU Court of Justice in order to challenge the relevant EU measures (decisions and regulations), whether they are autonomously adopted by the EU or adopted by the EU in line with UNSCR 1373.

*At national level*, no publicly known procedure is available for the revision of the designation decision. The authorities refer to a vague provision about application of a petition, which, however, does not provide any reference to de–listing, un–freezing of assets, or other measures under the UNSCR 1373. This is not sufficient, especially since Croatia does not have any national framework for implementation of UNSCR 1373.

(d) and (e) With regard to designations under 1267/1989 and 1988, designated persons/entities are informed of the listing, its reasons and legal consequences, their rights of due process and the availability of de–listing procedures including the UN Office of the Ombudsperson (UNSCR 1267/1989 designations) or the UN Focal Point mechanism (UNSCR 1988 designations). *At EU level,* there are procedures that provide for de–listing names, unfreezing funds and reviews of designation decisions by the EU Council (EU Regulation 753/2011, Art.11; EU Regulation 881/2002, Art.7(a)(e)). *At national level*, there is no formal procedure.

(f) *At EU level*, upon verification that the person/entity involved is not designated, the funds/assets must be unfrozen (EU Regulations 881/2002, 753/2011 and 2580/2001). The EU Best Practices on the implementation of restrictive measures provide guidance on the procedure for cases of mistaken identity (see para–s 8–17). *At national level*, no additional information was provided by the authorities on national procedures for unfreezing in case of false positives.

(g) *At EU level*, legal acts on de–listing are published in the EU *Official Journal* and information on the de–listings is included in the Financial Sanctions Database maintained by the European Commission (EU Regulation 881/2002, Art.13; 753/2011, Art.15; 2580/2011, Art.11).

*At national level*, according to IRM Law (Art.10(4)), the MFEA provides on its webpage a list of the natural and legal persons and other entities subject to EU and UN restrictive measures. Apart from this, and the notification to the entity against whom the asset freezing measure has been implemented by the REs stated under Clause 8 of the Guidelines for the Implementation of Restrictive Measures Against Asset Disposal Pursuant to the IRM Law, no further information or guidance is provided on ensuring timely communication of de–listings and unfreezing to FIs and DNFBP sectors, and defining their obligations to respect a de–listing or unfreezing actions.

***Criterion 6.7*** – *At EU level*, there are procedures in place to authorise access to frozen funds or other assets which have been determined to be necessary for basic expenses, for the payment of certain types of expenses, or for extraordinary expenses: EU Regulation 881/2001, Art.2(a); EU Regulation 753/2011, Art.5; and EU Regulation 2580/2001, Art.5–6.

*At national level*, IRM Law (Art.12) regulates the process by defining that the competent court may allow the frozen assets and other property to be released or be available by informing about the approval to the MFEA, which in turn informs the relevant international bodies.

*Weighting and Conclusion*

Croatia has made efforts to meet the lacunae highlighted in the 4th round MER by adoption of amendments into IRM Law, but shortcomings remain. This is mainly a considerable reliance placed on the EU mechanisms with no sufficient national mechanisms set for implementation of these UNSCRs. This affects compliance of Croatia with identifying and designating persons and entities under the UNSCR 1267/1989, 1988, 1373; timely implementation of the UNSCRs; coverage of assets to freeze and or make available; communication of designations, provision of guidance; reporting of attempted transactions; protection of bona fide third parties; lack of publicly known procedures for de–listing and unfreezing of funds and assets. **R.6 is rated PC.**

### *Recommendation 7 – Targeted financial sanctions related to proliferation*

The previous mutual evaluation of Croatia was conducted prior to the adoption of R. 7. The legal basis for implementing R.7 includes relevant EU legislation, and at the national level, the IRM Law. The same national legal provisions are applicable regarding TFS on TF, as well as on PF.

***Criterion 7.1*** – The UNSCRs related to the prevention, suppression and disruption of PF and its financing are implemented in the EU Regulations 2017/1509 (DPRK) and 267/2012 (Iran), as amended[219]. In the EU legal framework, EU Regulations are directly applicable in EU Member States. Nevertheless, the existing EU implementation process does not meet the essential requirement to implement UNSCRs without delay. While the sanctions for DPRK are generally not implemented "without delay", the sanctioning system (similar to the system for Iran) is also mitigated by the significant number of other designations by the EU. With regard to Iran, the technical problems in the EU for the transposition of UN sanctions and any delays which might have occurred in Croatia after such transposition have not, in practice, led to any delays in the implementation of TFS related to PF. *At the national level*, there is no explicit provision related to the implementation of TFS "without" delay.

***Criterion 7.2*** – IRM Law (Art.5(1)) establishes the Standing Group headed by the Ministry as a responsible authority for monitoring and coordinating of the implementation of restrictive measures under the IRM Law.

(a) *At the EU level,* the relevant EU Regulations require all natural and legal persons within the EU to freeze the funds or other assets of designated persons and entities. This obligation is triggered as soon as the regulation is approved and the designations are published in the EU *Official Journal*.

*At the national level,* natural and legal persons and other entities to freeze the assets and other property (IRM Law, Art.11(a)). The assets and other property of entities against whom the restricted measures are implemented shall be frozen without prior notification/announcement to the entities (IRM Law, Art.11(1(d)). According to Item 2 of the Government decision on the

[219] As regards the DPRK, UNSCRs 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 and 2321 (2016) have been transposed by Council Decision 2016/849/CFSP and Council Regulation 2017/1509, both as amended. As regards Iran, TFS imposed by the UN are mainly established by Council Decision 2012/35 and Regulation 267/2012. With the adoption of UNSCR 2231 (2015), which terminated UNSCR 1737 and its successor resolutions, a number of targeted restrictive measures contained in EU Regulation 267/2012 have been lifted.

manner of implementing international measures to restrict the disposal of property (OG 1651/2011), all assets defined under IRM Law (Art.3) shall be frozen without delay.

(b) *At the EU level,* under the EU framework, the obligation to freeze funds extends to all types of funds or other assets as stipulated under the FATF Standards.

*At national level*, the freezing obligation extends to the funds and other assets as described in the analysis for c.6.5 (b). This does not cover a sufficiently broad range of assets as provided under the FATF Standards.

(c) *At the EU level,* EU nationals and persons within the EU are prohibited from making funds and other assets available to designated persons and entities unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU Regulations 329/2007 (Art.6(4)) and 267/2012 (Art.23(3)).

*At the national level*, IRM Law (Art.(11(1(b)) prohibits making the assets available, directly or indirectly, to the entity against which the measures are applied, and persons acting on behalf or for the account of the entity may not control or have them in their possession. IRM Law (Art.11(1(b)) set out a national framework for prohibitions.

(d) The mechanisms described in c.6.5 (d) apply for communicating designations to FIs and DNFBPs and providing guidance.

(e) *At the EU level*, FIs and DNFBPs must immediately provide to the competent authorities all information that will facilitate observance of the EU Regulations, including information about the frozen accounts and amounts (EU Regulation 2017/1509, Art.50 and EU Regulation 267/2012, Art.40).

*At national* level, there is a general requirement to notify the MFEA on the application of restrictive measures (IRM Law, Art.10(1)). No requirements are in place for reporting attempted transactions.

(f) The rights of bona fide third parties are protected at European level (EU Regulation 2017/1509, Art.54 and EU Regulation 267/2012, Art.42).

*At national levels*, there is no specific rule for the protection of *bona fide* third parties acting in good faith when implementing the obligation under UNSCRs.

***Criterion 7.3*** – *At the EU level*, Member States are required to take all necessary measures to ensure that the EU Regulations on this matter are implemented and to determine a system of effective, proportionate and dissuasive sanctions in line with EU Regulations 329/2007 (Art.14) and 267/2012 (Art.47).

*At the national level,* The IRM Law (Art.13) envisages that supervision of implementation of this Act and regulations passed on the basis thereof shall be carried out by competent state administrative bodies and bodies vested with public powers in charge of the area to which the restrictive measures refer. The IRM Law (Art.14–16) provide sanctioning measures for non–compliance with the provisions of the Law, which are, however, not proportionate and dissuasive. Further on the Government Decision "On Determination of State Administration Bodies […] of the Implementation of International Restriction Measures Determined by Legal Acts of the EU empowers the CNB, the CFSSA, Financial Inspectorate and the TA respectively with supervision of implementation of measures under the EU, but not the UN framework. Hence, the framework would be applicable only to the extent to which the listed persons would match.

***Criterion 7.4*** – Croatia does not have publicly known procedures for de–listing.

(a) The EU Regulations contain procedures for submitting de–listing requests to the UN Security Council for designated persons or entities that, in the view of the EU, no longer meet the criteria for designation. Where the UN de–lists a person/entity, the EU amends the relevant EU Regulations accordingly. *At national level*, no publicly known procedure is available for the revision of the designation decision. The authorities refer to a vague provision on application of a petition, which, however, does not provide any reference to de–listing measures under the UNSCRs.

(b) Publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities are provided for at EU level. *At national level*, no additional information was provided by the authorities on national procedures for unfreezing in case of a false positive match.

(c) *At the EU level*, there are procedures for authorising access to funds or other assets if Member States' competent authorities have determined that the exemption conditions of UNSCRs 1718 and 1737 are met (EU Regulation 329/2007, Art.7; EU Regulation 267/2012, Art.26–28). *At national level*, relevant provisions are stipulated under IRM Law (Art.12).

(d) See 6.6 (g).

***Criterion 7.5*** – (a) *At the EU level*, the addition of interests or other earnings to frozen accounts is permitted pursuant to EU Regulation 2017/1509, Art.36 and EU Regulation 267/2012, Art.29). *At the national level*, IRM Law (Art.11(2–3)) states that crediting frozen accounts with interest or other incomes, or funds transferred by a third person shall not be prevented, provided that all such inflows shall also be frozen. However, there is no provision specifying the payments due under contracts, agreements, or obligations should have been raised prior to the date on which the property became subject to freezing.

(b) *At the EU level*, making payments under a contract entered into prior to designation are possible under the necessary conditions (EU Regulation 2015/1861, Art.25, which amends EU Regulation 267/2012). *At the national level*, no specific provision was provided.

*Weighting and Conclusion*

Croatia implemented measures with respect to PF on TFS by adoption of amendments into IRM Law, but shortcomings remain. This is mainly due to a considerable reliance placed on the EU mechanisms with no sufficient national mechanisms set for implementation of these UNSCRs. Technical deficiencies are similar to ones described in R.6. In addition, at national level, deficiencies are noted with the scope of supervisory coverage and regulation of additions to or payments from frozen accounts. **R.7 is rated PC**.

### *Recommendation 8 – Non–profit organisations*

In the 4th round MER of 2013, Croatia was rated PC with the former SR.VIII due to the absence of a comprehensive domestic review of the non–profit organisations (NPO) sector's vulnerabilities, insufficient outreach to the NPO sector, including little awareness–raising on the risk of NPOs to be misused for TF, deficiencies in the information maintenance period. The exit follow–up report noted that in the analysis under SR.VIII, all technical deficiencies identified in the 4th round MER had been addressed. Nevertheless, since the adoption of the 2013 MER, R.8 has changed significantly.

***Criterion 8.1*** – (a) The NPO sector was considered within the scope of the two NRAs conducted in 2016 (subject to ML vulnerabilities in the sector) and 2020 (as a variable for assessment of the Country's TF vulnerabilities). In addition, Financial Inspectorate conducted a thematic analysis of business operations of foreign foundations and associations operating in Croatia in 2019 for the purpose of ML and TF risk assessment. None of these exercises led to identification of the subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse by virtue of their characteristics. (See also analysis in IO.10)

(b) Croatia has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk, as well as how terrorist actors abuse those NPOs.

(c) Croatia has not reviewed the adequacy of measures, including laws and regulations that relate to the subset of the NPO sector that may be abused for terrorism financing support.

(d) The assessment of the NPO sector is conducted within the scope of the NRA. The AMLTFL sets out the legal requirement for Croatia to carry out the NRA every four years, or earlier if deemed necessary (Art. 5 (1)).

*Sustained outreach concerning terrorist issues*

***Criterion 8.2*** – (a) The Financial Operations and Accounting of Non–Profit Organisations Law (FOA NPOs Law) was adopted in 2014, which envisages essential requirements for NPOs related to the financial operations and accountancy, financial management system, preparation and execution of financial plans, business records, double–entry bookkeeping principle, list of assets and liabilities, principles of declaring asset, commitments and own resources, principles of recognising revenues, expenditures, receipts and expenses, financial reporting, publication of audit reports and annual financial statements, supervision of financial transactions and accounting (Chapters I–V, VIII, IX of the FOA NPOs Law). The Register of NPOs is a central source of data on NPOs necessary for the determination and monitoring of the obligation of preparing and submitting financial statements, determining their financial position and business operations and earmarked use of budget funds. This electronic register is maintained by the MoF. It is not clear that any other measures have been taken to promote public confidence in the administration and management of NPOs.

(b) The AMLO organises the Annual Conference on the Prevention of ML and TF in co–operation with the Croatian Chamber of Commerce for REs, supervisory bodies, other competent authorities with participation of representatives of associations. However, considering that the TF risks in the NPO sector are not identified, this outreach does not seem to be targeted. No steps were taken to raise awareness of the NPOs on measures that they can take to protect themselves against such abuse has been undertaken.

No outreach and educational programmes to raise and deepen awareness among the donor community on the potential vulnerabilities of NPOs to TF abuse and TF risks.

(c) No steps have been taken by the authorities on co–operation between competent authorities and the NPO sector in developing and refining best practices to address TF risks.

(d) Natural and legal persons carrying out a registered activity are not allowed to receive a payment or to carry out the payment in cash in the amount of HRK 75 000 (EUR 10 000) or more. The restriction also applied to smaller linked transactions. Funds should be paid through or transferred to the account opened at a credit institution (AMLTFL, Art.55). This restriction also applies to NPOs, in effect serving as an encouragement for use of regulated financial channels

when transacting funds equal and higher than the set threshold. This, however, does not cover scenarios of transactions below the cash threshold.

*Targeted risk–based supervision or monitoring of NPOs*

***Criterion 8.3*** – Croatia applies a one–size–fits–all approach to supervision of the NPO sector. NPOs are obliged to maintain financial management system, business records, double–entry bookkeeping principle and other requirements related to the financial operations and accountancy stated under c.8.2a. Annual financial statements of NPOs shall be published on the Register of NPOs. In addition, bookkeeping documents, business records and financial statements should be kept in a way, which enables the verification of transactions, determination of financial position and business operations of the NPOs.

The Department for financial and budgetary supervision of NPOs and other legal and natural persons of the MoF carries out supervision of the NPOs, which comprises *inter alia* the supervision of lawful collection of funds from public and other resources, management of funds and determination if the funds are used consistent with the purpose and objective of the NPOs stated activities (FOA NPOs Law, Art.38).

Supervision includes inspection at the supervised person, analysis of business documentation, regulations and general acts in line with which the supervised person operates, examination of business premises, buildings, objects, goods and other stuff, monitoring, collection and verification of bookkeeping documents, business records and financial statements, as well as verification of the system the supervised person uses for data processing regarding the accounting activities (FOA NPOs Law (Art.39).

However, in addition to the lack of risk–based supervision, Croatia also does not apply to NPOs measures foreseen under para. 6b(v)of INR.8.

***Criterion 8.4 –*** (a) Monitoring, collecting and verifying bookkeeping documents, business records and financial statements are part of the supervision performed by the MoF. Information is referred to the competent SAO and TA whenever NPOs' actions raise suspicions on criminal matters or tax misdemeanour, accordingly. However, there is no monitoring of risk–based measures applied to NPOs, and this supervisory exercise does not have a targeted approach.

(b) The FOA NPOs Law prescribes sanctions for NPOs and their legal representatives for failing to comply with requirements of the Law. These, however, do not amount to sanctions that are set and relevant to implementation of risk–based measures, specifically, and would have an indirect application only. In the framework of the supervision, supervisor is authorised to order the removal of irregularities and set the deadline for addressing deficiencies. A fine up to EUR 26 538 can be imposed on the legal representative of an NPO for a misdemeanour of the provisions stated under FOA NPOs Law, Art.45. Various criminal sanctions, including fines, imprisonment, preventative measures such as prohibition of performing certain activities, confiscation can be imposed on the NPOs and their legal representatives prescribed by the Liability of Legal Persons for Criminal Offences Law.

A fine up to EUR 1 328 can be imposed on the institutions, and a fine up to EUR 664 – to the responsible person, in particular, when the institution performs an activity that is not entered in the court register or the profits are not used for the performance and development of the activities of the institution in accordance with the founding act and the statute (Institutions Law, Art.77). In addition, the term of dissolution and liquidation of the association on the basis of a court decision or other conditions is provided under Associations Law, Art.48.

**Criterion 8.5** – (a) Co–operation, coordination and information sharing among all the competent authorities, including the SAO, MoF, and AMLO, is carried out within the scope of IIWG (AMLTFL, Art. 120(2)). The MoF also should co–operate with: (i) AMLO, in case of detection of ML/TF suspicion (AMLTFL, Art. 89(2) and FOA NPO Law, Art.44(5); (ii) SAO and TA, whenever NPOs' actions raise suspicions on criminal matters or tax misdemeanour (NPO Law (Art.44(3–4)). In addition, the AMLO should deliver to the MoF data on cash transactions and transfers of cash across the state border for supervision and financial investigation purposes (AMLTFL, Art.124).

Most information concerning NPOs is available online at https://banovac.mfin.hr/rnoprt/[220]. BO information of the associations and foundations held with the BO Register is directly accessible from January 2020. In electronic form, this information is accessible also to all competent authorities.

(b) The Counter Terrorism Department (CTD) of the Police National Office for Suppression of Corruption and Organised Crime (PNUSKOK) and County SAOs are the designated authorities for preventing, detecting and investigating terrorism and other terrorism–related crimes. There is no specific investigative expertise to examine NPOs suspected of TF, but Croatia applies all respective LEA general powers and tools that the latter are provided with and are in possession of, to enable the investigation of NPOs suspected of TF abuse. So far, no links of NPOs to terrorist groups or organisations, terrorism–related individuals or terrorism financing by exploiting or abusing their capabilities have been detected.

(c) There are various gateways available for CTD and the County SAOs to obtain information on the administration and management of NPOs. Most information concerning NPOs, as well as BO information of the associations and foundations are available in the NPOs and BO Registers. Additionally, information can also be obtained from the MoF, AMLO and TA. In the course of a criminal investigation, information on a legal person is available to a police officer on the basis of the powers described under the PDPL (Art.71). Thus, there are no restrictions for access to information kept by the NPOs.

(d) There are multiple measures in place in Croatia that would ensure prompt notification to the competent authorities when there is a suspicion that the NPO is abused for TF or involved in any way, as described in the criterion. In the framework of NPO supervision, in case of suspicion of ML/TF, the MoF is obliged to notify this to: (i) AMLO, in case of detection of ML/TF suspicion (AMLTFL, Art. 89(2) and FOA NPO Law, Art.44(5); (ii) SAO, whenever NPOs' actions raise suspicions on criminal matters. In addition, REs should file STR to the AMLO in case of TF suspicion, including when the NPO is concerned. The AMLO shall submit the results of its operational analyses and all other relevant information to the competent authorities (Police and SAO) for further action when TF suspicion is detected.

*Effective capacity to respond to intentional requests for information about an NPO of concern*

***Criterion 8.6*** – Croatia has not identified specific points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support. Croatia relies upon existing mechanisms for

[220] Information related to the foundations and associations can also be obtained from the Register of Foundation available at https://registri.uprava.hr/#!zaklade link and from the Register of Association available at https://registri.uprava.hr/#!udruge link. Additionally, information on the companies and institutions are available in the Court Register available at https://sudreg.pravosudje.hr/registar/f?p=150:1 link.

international co–operation (via MLA, Interpol–Europol–S.I.Re.N.E., FIU–to–FIU and other means for communication).

*Weighting and Conclusion*

The NPO sector is conducted as part of the NRA, which did not lead to identification of the NPOs at TF abuse risk. Other analyses are mainly aimed at increasing transparency of the sector, but no in–depth assessment of their risks for TF abuse has taken place, the nature of threats is not identified, and adequacy of measure is not reviewed. Weaknesses are present in ensuring the elements of sustained outreach concerning TF issues in the NPO sector. Supervisory measures in place are not risk–based and are directed to tax compliance matters rather to compliance of NPOs with implementation of R.8 requirements. General information gathering and investigation mechanisms are in place. **R. 8 is rated PC**.

### *Recommendation 9 – Financial institution secrecy laws*

In the 4th round MER of 2013, Croatia was rated LC on R.4. The main deficiencies identified were related to the following: the Leasing Law requirement on the data confidentiality inhibited information sharing in cases of TF; it was unclear whether credit institutions are allowed to share CDD information about their clients with their correspondent banks; no special provision in the AMLTFL that the contract for the correspondent banking relationship should determine a correspondent bank's ability to submit the data gathered in the course of identification and verification of the customer based on an enquiry; and the lack of clarity on whether the banking secrecy regulations can inhibit the implementation of R.4.

***Criterion 9.1*** – The Croatian legal framework provides for the obligation of the CNB, Financial Inspectorate, the CFSSA, the AMLO, SAO, LEAs, TA, Customs Administration (CA) and other competent authorities to access and use the confidential information they have received exclusively for the purpose for which it has been given and may not divulge it to third parties or enable third parties to acquire and make use of such information, except in cases prescribed by the law.

*(a) Access to information by competent authorities*

Delivery of data, information and documentation, including customer information to the AMLO does not represent a disclosure of business and/or professional secrecy (AMLTFL, Art. 77(4(1)). The prohibition of disclosure of business and/or professional secrecy does not apply if data, information and documentation, collected and kept by REs are necessary for: (i) criminal proceeding, upon the request by the competent Court; (ii) supervisory purposes (AMLTFL, Art.74(4(1–2)).

In addition, access to FIs secrecy data is regulated by the sectorial legislation that contains similar provisions, as follows: the obligation of a Credit Institution to maintain banking secrecy does not apply when confidential information is communicated to the CNB, the Financial Inspectorate, the AMLO, the SAO, USKOK, MoI, or the TA and CA and other competent authorities (Credit Institutions Law, Art.157(3)3,10,11,12, 21). Similar provisions are prescribed for FIs by the Factoring Law (Art.102(2)), the Leasing Law (Art.108(2)), the Voluntary Pension Funds Law (Art.308a(3)1), the Capital Market Law (Art.400(3)1), the Open–Ended Investment Funds with a Public Offering Law (Art.389(2)1), the Alternative Investment Funds Law (AIF) (Art.281(2)1), the Law on open investment funds with public officers (Art.389(2)1) and the Insurance Law (Art.387(2)2), Pension Insurance Companies Law, Art.68(3)).

*(b) Sharing of information between competent authorities domestically and internationally*

The transfer of information from the AMLO to relevant domestic authorities and foreign counterparts constitutes classified and confidential data. The disseminations of such data do not constitute a breach of such confidentiality (AMLTFL, Art. 129, 138). Information exchange with domestic authorities upon AMLO's request and access to electronic data, including classified information, is regulated under the AMLTFL, Art. (Art.115(1) & 116(2)).

Sectorial legislation provides a regulatory framework for sharing of information that constitutes secrecy between competent authorities. The CNB may communicate confidential supervisory information to the Financial Inspectorate, the TA, and the AMLO (as structural units of the MoF), the CFSSA and the LEAs (Credit Institutions Law, Art.211). At the request of an individual competent authority, the CFSSA shall submit to that authority all data on supervised entities required in the supervision procedure. Such sharing of information shall not constitute a disclosure of confidential information (Capital Market Law, Art.392). Similar provisions allow the CFSSA to share confidential information stemming from other FIs with investigative bodies (Law on Voluntary Pension Funds, Art.308b(4), Insurance Law, Art.397(6)). The obligation to keep business secrets and classified information has not been violated if the data is provided for the purposes of criminal proceedings if it is provided to the AMLO or another supervisory body for the purposes of supervision (Financial Inspectorate Law, Art.36(4)).

As regards international co–operation, the supervisory authorities shall co–operate and exchange information with competent supervisory authorities of EU Member States (AMLTFL, Art.90) and competent authorities of non–EU Member States upon signature of a co–operation agreement (AMLTFL, Art.92).

LEA's power to obtain information, including that which constitutes secrecy, can be accessed from the other competent authorities on the basis of the legislative provisions as indicated above and the general competences provided by the CPC. As concerns international co–operation, such data may exchange based on the requests from EU foreign bodies conducting the criminal investigation (Judicial Co–operation in Criminal Matters with the EU Member States Law (JCCMEUL), Art.6(1) and 7(1)). LEAs exchange information with non–EU counterparts through INTERPOL and bilateral agreements.

*(c) Sharing of information between financial institutions*

The prohibition of exchange of classified information, including personal data by REs, shall not apply when this information is exchanged within the same group and category of REs (AMLTFL, Art.75 and 76). As such, the law does not impose any restrictions that would complicate information sharing under R-s.13, 16, 17.

The obligation of a credit institution to maintain banking secrecy shall not apply if confidential information is exchanged within the group of credit institutions or if it is communicated directly to another credit institution (Credit Institutions Law, Art.157(3)4,5).

*Weighting and Conclusion*

The financial institution secrecy laws in Croatia do not inhibit implementation of the FATF Standards, providing for the possibility of competent authorities to access and share information domestically and internationally, as well as to share information between FIs. **R.9 is rated C.**

### *Recommendation 10 – Customer due diligence*

In the 4th round MER of 2013, Croatia was rated PC with former R.5. The main technical deficiencies identified related to the application of exemptions and derogations from CDD obligations such as the postponement of all CDD measures in certain exceptional cases; SDD was permitted in relation to all foreign financial institutions regardless of their level of compliance with the FATF Standards; FIs were not required to obtain information on the entity or directors for foreign entities and arrangements. All the technical deficiencies identified in the 4th Round MER were subsequently addressed by Croatia with the revised AMLTFL, and in accordance with the progress report of July 2019, Croatia was re–rated as compliant with former R.5. Since then, the FATF Standards for CDD have substantially changed.

***Criterion 10.1*** – After the entry into force of the AMLTFL in 2019, FIs are not allowed to open, issue or keep anonymous accounts, coded or bearer passbooks, anonymous safe deposit boxes, or other anonymous products, including accounts on false names, which would indirectly or directly enable the concealment of the customer's identity (AMLTFL, Art.54(1)). This provision, however, allows anonymous accounts, passbooks, safe deposit boxes or other anonymous products that existed as of 2019 to continue until such time as possible to remediate and in any case prior to any use thereof, the effect of which is to freeze the account (AMLTFL, Art.54(2)). Upon occurrence of a trigger event, FIs that cannot fulfil CDD requirements shall terminate already established business relationship (AMLTFL, Art.19(1)).

***Criterion 10.2*** – FIs shall conduct CDD in the following circumstances: (i) when establishing a business relationship with a customer, (ii) when carrying out an occasional transaction amounting to HRK 105 000 (EUR 14 000) or more, regardless whether that transaction is carried out in a single operation or in several transactions that are apparently linked, (iii) when carrying out an occasional transaction constituting a transfer of funds as per EU Regulation 2015/847 which exceeds EUR 1 000, (iv) when there are reasons for suspicion of ML/FT in relation to a transaction or a customer, regardless of all prescribed exemptions and the transaction value, and (v) when there are doubts about the veracity or adequacy of the previously obtained data on a customer (AMLTFL, Art.16(1)). The obligation to carry out CDD measures in the circumstances outlined above is subject to conditions laid down in the AMLTFL and regulations passed pursuant to this (AMLTFL, Art.16(1)), however, the conditions are not defined.

Authorised exchange offices are required to identify and verify the identity of customers when they carry out transactions above HRK 15 000 (EUR 2 000) (AMLTFL, Art.16(2)). While the Croatian authorities read the legislative provision as a requirement to conduct CDD, the wording of the AMLTFL creates legal uncertainty as to whether authorised exchange offices are required to implement all the CDD measures (and not merely identification and verification of identity of customers).

***Criterion 10.3*** – CDD measures shall include the identification of the customer and the verification of the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source (AMLTFL, Art.4(46), 15(1(1)). Art. 20, 21, 23 of the AMLTFL then provide further details on the identification and verification of identity procedures that need to be implemented for the various types of customers, including natural and legal persons.

There is no explicit provision for the identification and verification of customers that are foreign trusts or similar legal arrangements since the definition for customer refers only to persons. REs have to collect data on the legal arrangement of the trust or similar arrangement and its

memorandum of association, this, however, does not amount to requiring the identification and verification of a foreign trust or similar legal arrangement (AMLTFL, Art. 31(3)).

***Criterion 10.4*** – REs should identify and verify a person claiming to act on behalf of a customer (AMLTFL, Art. 15(2)). Identification and verification measures to be carried out on representatives of natural and legal persons are stipulated under AMLTFL, Art. 22, 24–25. These provisions, however, (1) do not explicitly cover persons that would be acting on behalf of foreign trusts or similar legal arrangements since the definition for customer refers only to persons, and (2) do not contemplate scenarios where customers might be represented by legal persons.

It is not clear that the legislation requires the RE to verify that any person purporting to act on behalf of a customer is authorised to do so. This is because the obligation arises only when a person "claims" to act on behalf of a customer and not when the RE collects this information from the customer or otherwise (AMLTFL, Art.15(2)).

***Criterion 10.5*** – The identification of the customer's BO and the taking of reasonable measures to verify the BO's identity is part of the CDD (AMLTFL, Art.15(1(2)). Measures to gather information on and identify the customer's BO are prescribed under AMLTFL, Art.30–31. The definition of BO is broadly in line with the FATF definition.

The legal uncertainty explained in c.10.2 puts into question whether authorised exchange offices are bound to identify and verify the BO of a customer (AMLTFL, Art. 15(1), 16(2)).

***Criterion 10.6*** – CDD measures include the collection of data on the purpose and intended nature of the business relationship or a transaction (AMLTFL, Art.15(1(3)). REs are, however, not required to also understand the purpose and intended nature of the business relationship.

The legal uncertainty explained in c.10.2 puts into question whether authorised exchange offices are bound to implement the provisions of AMLTFL, Art.15(1(3) and obtain information on the purpose and intended nature of the business relationship or transaction.

***Criterion 10.7*** – Ongoing monitoring of the business relationship is stipulated in AMLTFL, Art.15(1(4) and 37. The scope and frequency of on–going monitoring measures shall be adapted to the ML/TF risks. On–going monitoring includes:

(a) the scrutiny of transactions carried out during the course of the business relationship, to ensure that these transactions are consistent with the RE's knowledge of the customer, type of business and risk profile, including, where necessary, the collection of information on the source of funds.

(b) ensuring that the documents and the data held by the RE are kept up–to–date.

However, the keeping of CDD documents and data up to date is occasioned by or ancillary to, the on–going scrutiny of transactions and does not form a distinct process of reviews of existing CDD records. In addition, the requirement does not extend to the monitoring and updating of all CDD documents, data or information obtained, but those that pertain to the customer, BO and/or related to the customer risk profile (AMLTFL, Art.15(1(4), 37(2)).

***Criterion 10.8*** – CDD shall include the taking of measures necessary to understand the ownership and control structure of the customer when the customer is a company, another legal person or foreign trust or similar arrangement (AMLTFL, Art.15(1(2)). There is no explicit requirement for REs to understand the nature of the customer's business. However, FIs are mandatorily required to consider the risks related to the customer's and the customer's BO's business or professional

activity (CNB and MoF Ordinance[221], Art.11(1), CFFSA Ordinance, Art.8(1)). These provisions, indirectly rather than explicitly, require REs to obtain information on and, to a certain extent, understand the customer's business.

***Criterion 10.9*** – The requirements to identify and verify legal persons, other types of legal persons, and foreign legal arrangements are set out in AMLTFL, Art. 20(1(1(4b), (1(4)), Art.23, Art.26 and Art.31.

*(a) name, legal form and proof of existence*

REs should identify and verify the identity of customers that are legal persons by collecting the name, legal form, headquarters address and business registration number of the legal person by examining the original or notarised copy of documentation from the court or other public register or by directly examining such court or public register. Similar provisions are set for other types of legal persons (namely NGOs, funds, foundations, institutions, artistic organisations etc.), with the requirement to examine the register, record files, or other official records.

Proof of existence for legal persons is established through the collection of information and reference to court and public registers outlined above. Moreover, in the case of other types of legal persons, REs should examine registers and record files, however, it is not made clear what registers and record files the law is referring to.

For trusts and similar entities setup under foreign law, REs should collect data on such trust or similar entity and obtain the memorandum of association (presumably the trust deed or similar document) of that trust or similar entity. REs are thus not explicitly required to obtain and verify the name, legal form and proof of existence.

*(b) the powers that regulate and bind the legal person or arrangement, and names of senior management*

REs are not required to obtain information on the powers that regulate and bind the legal persons. In the case of foreign trusts and similar legal entities, REs are required to collect the memorandum of association of the trusts or similar entity (presumably the trust deed or similar document), which would contain information on the powers that regulate and bind that legal arrangement. However, similarly, there is no clear requirement for REs to obtain such information.

REs should collect data on the management board or persons performing equivalent functions (name, surname, identification number, country of residence) and data on persons authorised to represent the legal entity (name, surname, identification number, country of residence). However, this is only applicable to foreign legal persons, and thus there are no similar requirements for all types of legal persons incorporated in Croatia.

In the case of foreign trusts and similar legal entities, REs are required to establish and verify the identity of trustees, protectors, or any other person that has ultimate control over that trust or similar legal entity.

*(c) address of the registered office and, if different, a principal place of business*

REs should obtain information on the headquarters of legal persons, which would include the street and number, place and country.

[221] Ordinances "On the Assessment Procedure of the ML/TF Risk and on the Manner of Applying Simplified and Enhanced Customer Due Diligence Measures" issued by the CNB, Financial Inspirate and the CFSSA

In the case of foreign trusts and legal arrangements, whilst there is no explicit requirement to collect information on the country of establishment, this would be contained in the memorandum of association (presumably the trust deed or similar document), which REs are required to obtain. REs should obtain information on the residential address of the trustee as beneficial owner.

***Criterion 10.10*** – REs should identify the customer's BO and take reasonable measures to verify the BO's identity (AMLTFL, Art.15(1(2)). REs shall take measures to identify the BO of legal persons, foreign trusts and similar arrangements, and verify his identity, as provided in the AMLTFL, Art.30–31.

BO is defined as any natural person who ultimately owns the customer or controls the customer or in any other way manages it, and/or any natural person on whose behalf the transaction is being conducted, including a natural person who exercises ultimate effective control over a legal person or legal arrangement (AMLTFL, Art.4(42)). This is then complemented by a more detailed definition of the term beneficial owner(s) with respect to legal persons, legal arrangements and individuals acting on behalf of or controlling other natural persons (AMLTFL, Art.28).

*(a) the natural person(s) who ultimately has a controlling ownership interest in a legal person*

In the case of legal persons, the BO shall include: (i) a natural person who owns or controls a legal person through direct ownership via a sufficient percentage of stocks or shares of voting rights or ownership shares in that legal person and (ii) a natural person who controls a legal person through indirect ownership via a sufficient percentage of stocks or shares of voting rights or ownership shares in that legal person. Direct ownership is defined as the ownership of more than 25% of the ownership shares, voting or other rights, which enable one to manage the legal person or the ownership of 25% plus one of the shares. Indirect ownership is defined as the ownership or control over one or more legal persons which individually or together have more than 25% of the business shares or 25% plus one share in the corporate customer (AMLTFL, Art.28(1(1–2), 5–6).

However, indirect ownership does not include ownership or control of the customer through one or more legal arrangements (but only through legal persons) and does not include ownership or control of legal persons or arrangements that (individually or together) may control the customer through ownership of 25% or more of the voting rights.

*(b) where there are doubts or there is no beneficial owner in terms of (a); the natural person(s) exercising control through other means*

In the case of legal persons, the BO shall also include a natural person(s) who has a controlling function in managing the legal person's property via other means (AMLTFL, Art.28(1(3)). Indication of what control via other means may constitute is stipulated under AMLTFL, Art.28(7).

*(c) where no natural person is identified under (a) or (b); the natural person(s) holding the position of senior managing officials*

Where all possible means have been exhausted, but it is not possible to identify the BO, or there are suspicions that the identified natural person(s) is not the BO, the natural person(s) who is a member of the management board or other managing body or a person performing equivalent functions is to be considered as the BO. REs should keep records of measures taken and any difficulties encountered during the verification of the BO process (AMLTFL, Art. 28(8)).

When it is not possible to identify the BOs, REs should consider the natural person authorised to represent the entity as the BO (AMLTFL, Art.28(4)).

***Criterion 10.11*** – BOs of trusts and similar entities, which are set up under the law of a foreign jurisdiction, are defined under AMLTFL, Art.31(1).

*(a) for trusts: the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust*

For trusts, REs are required to establish and verify the identity of all settlor(s), trustee(s), protector(s) if any, beneficiaries or class of beneficiaries (as applicable), persons performing equal or similar functions, and all other natural persons who, via direct or indirect ownership or by other means ultimately perform the ultimate control over the trust (AMLTFL, Art. 31(1)). Were any of the mentioned persons are legal persons, the RE shall identify and verify the identity of their BOs.

If the beneficiary of a trust is designated by characteristics or class, REs are required to collect sufficient information to establish the identity of the beneficiary at the moment of the payout or when the beneficiary intends to exercise its vested rights (AMLTFL, Art.16(5)).

*(b) for other types of legal arrangements: the identity of the persons in equivalent or similar positions*

The provisions set out in sub–criteria (a) are applicable to other types of legal arrangements subject to limitations since the term "trust" is defined to include express *trusts, fiduciaries, treuhands, fideicommiso* and other similar legal forms of foreign law (AMLTFL, Art.4(51), (31)). Moreover, REs are likewise obliged to establish and verify the identity of all persons performing functions equal to or similar to the settlor, trustee, protectors and beneficiaries (AMLTFL, Art.31).

However, in view of the definition "trust", the regulatory framework described under sub–criteria (a) and (b) find application in respect of those trusts and similar legal arrangements that either: (i) have their trustee (or person performing similar functions) residing or seated in Croatia or (ii) that acquire real estate in Croatia or establish a business relationship with a Croatian RE (AMLTFL, Art.4(51), 31). Trusts or similar legal arrangements whose trustee (or person holding a similar function) resides in a foreign jurisdiction, or those trusts or similar legal arrangements that seek to carry out occasional transactions (excluding real estate occasional transactions) are not subject to the provisions of AMLTFL, (Art.31) fall outside the scope.

***Criterion 10.12*** – Insurance companies, agents and intermediaries, when entering into agreements on life insurance and other investment–related insurance, should carry out the following additional measures in relation to beneficiaries (AMLTFL, Art.16(3)): (i) identify and verify the beneficiaries' identity where these are determined and specifically appointed natural persons, legal persons or legal arrangements; and (ii) collect sufficient data to be able to identify the beneficiary at the moment of the policy payout, where the beneficiaries are determined by specific characteristics of class. REs are required to verify the identity of the insurance beneficiary at the moment of payout (AMLTFL, Art.16(4)).

Furthermore, The CFSSA's Ordinance[222] (Art.50(1–2)) clearly establishes that these requirements are applicable to all REs subject to these Ordinances, including insurance companies, agents and intermediaries.

[222] Ordinance "On the Assessment Procedure of the ML/TF Risk and on the Manner of Applying Simplified and Enhanced Customer Due Diligence Measures"

***Criterion 10.13*** – There is no explicit requirement for RE's to consider BOs as a risk factor when determining if EDD is required. However, there are various legal requirements that could implicitly mandate such. E.g.

(1) The CFSSA's Ordinance (Art.47(1)) requires REs to take into account a number of factors and behaviours related to customers of life insurance that may contribute to increasing risk. The factors or behaviours are not set in legislation, but examples are provided as guidance (such as whether the beneficiary is a PEP or a company with nominee shareholders or shares in bearer form).

(2) The CFSSA Ordinance (Art.49(1)) obliges REs to consider in their risk assessments whether the beneficiary or the BO of the beneficiary is linked to higher risk jurisdictions.

(3) The CFFSA's Ordinance (Art.51(1)) requires REs to carry out EDD measures in high–risk situations (which as explained may include risk factors linked to the beneficiary).

***Criterion 10.14*** –REs are obliged to identify and verify the customer and the BO and to collect information on the purpose and intended nature of the business relationship before establishing a business relationship or carrying out an occasional transaction. By way of derogation, REs are allowed to verify the customer's identity and the BO's identity during the establishment of a business relationship, and as soon as possible after the initial contact with a customer if: (i) it is necessary in order not to interrupt the normal conduct of establishing business relationships and (ii) there is a low risk of ML/TF (AMLTFL, Art.17(1, 3)).

These provisions, however, do not cover foreign trusts or similar legal arrangements since the definition for customer refers only to persons.

Within the context of the application of SDD, the delaying of the verification of customer and BOs is permitted even when this is not essential for uninterrupted conduct of business (AMLTFL, Art.43(3(1)), CNB and MoF Ordinances Art.19(3) and CFFSA Ordinance, Art. 15(3)).

***Criterion 10.15*** – Where REs apply the derogation explained under c.10.14, they should adopt written policies, controls and procedures for the mitigation and efficient management of risks. With regards to the delay of verification under the SDD framework (explained under c.10.4), there are specific risk mitigation and management measures to regulate cases where verification is delayed until transactions exceed a defined threshold or once a reasonable time limit has lapsed (CNB and MoF Ordinances, Art.19(3)(1(b)), CFSSA Ordinance, Art.(15(3)(1(b)).

These provisions, however, do not cover foreign trusts or similar legal arrangements since the definition for customer refers only to persons.

***Criterion 10.16*** – REs are required to carry out CDD measures on existing customers on the basis of the risk assessment, and particularly when the circumstances relevant for the application of the AMLTFL change in relation to particular customers. CDD on existing customers is also required to be carried out when the RE has a legal obligation (including under taxation legislation) to contact the customer to verify BO information (AMLTFL, Art.16(6)).

There is no specific requirement to take into account the adequacy of previously obtained CDD data, the timing of application of previous CDD when determining the appropriate times when CDD is to be carried out on existent customers, nor to consider materiality.

***Criterion 10.17*** – REs should conduct EDD measures to appropriately manage and mitigate the ML/TF risks where they estimate that the customer presents a high ML/TF risk (AMLTFL, Art.44(6)). Examples of high–risk scenarios are provided in AMLFTL (Art.14). Other situations in

which the application of EDD is mandatory, including also: cross–border correspondent relationships, dealings with PEPs, dealings with customers linked to high–risk non–EU Member States, dealings with customers that are legal persons having shares in bearer form, in cases of high ML/FT risks determined by the NRA, in cases of suspicions of ML/FT and in relation to complex and unusual patterns or types of transactions (AMLTFL, Art.44).

However, this falls short of the FATF Standards that require the application of EDD where there is a higher risk, and not just prescribed high–risk factors.

***Criterion 10.18*** – REs may conduct SDD if, according to their own risk assessment, they estimate that a customer represents a low ML/TF risk. REs should take into consideration the results of the NRA in making a determination on the level of risk (AMLTFL, Art.14(6), 43(1–2)).

Furthermore, the CNB, MoF and CFFSA Ordinances (Art.19(2) and Art.15(2)) applicable to all FIs have specific provisions which explicitly state that in case of low–risk business relationships and occasional transactions, the scope, timing or type of CDD may be adjusted in a way that is commensurate to that risk category.

SDD is not allowed in cases of suspicions of ML/TF or in specific scenarios of higher risk of ML/FT or in case of complex and unusual transactions (AMLTFL, Art.43(5)).

***Criterion 10.19*** – Where REs are unable to implement CDD (initial CDD, as well as on–going monitoring) they shall not be allowed to establish a business relationship, carry out a transaction, or shall have to terminate an already established business relationship. REs are also required to consider filing an STR. The Croatian authorities explained that the definition of the term business relationship encompasses the opening of accounts, however, there is no explicit provision prohibiting the opening of accounts if CDD has not or cannot be performed (AMLTFL, Art.4(31)).

***Criterion 10.20 (Not met)*** – There are no provisions that permit REs not to carry out CDD in case of suspicions of ML/TF and instead submit an STR if they reasonably believe that the carrying out CDD would tip off the customer.

*Weighting and Conclusion*

There are a number of CDD requirements implemented in Croatia, but these have certain gaps. The identification of BO is required to be risk–based, and indirect ownership only considers it through legal arrangements and does not include indirect ownership through legal persons; REs are not required to understand the purpose and intended nature of a business relationship; deficiencies in requirement for the collation of reliable information or data to assist in the verification of the identity of a BO, obtain information on the powers that regulate and bind the legal persons or legal arrangements, include the beneficiary of a life insurance policy as a risk factor in determining EDD measures, etc. There are some deficiencies on to the CDD requirements in respect to trusts and legal arrangements (foreign given these do not exist in Croatia), assessment of ongoing monitoring requirements for periodic reviews to ensure that CDD documents and data is up to date, no explicit provision that prohibits the opening of an account when CDD has not or cannot be performed. Legal uncertainties in measures applicable to Authorised exchange offices. This influences the rating. **R. 10 is rated PC.**

### *Recommendation 11 – Record–keeping*

In the 4th round MER of 2013, Croatia was rated LC on former R.10 on the basis of two main deficiencies: there was no requirement to prolong the record–keeping period upon request of a

competent authority and no regulation or guidance regarding the keeping of business correspondence. Since the last MER, Croatia adopted a new AMLTFL in 2018, which was subsequently amended in 2019.

***Criterion 11.1*** – FIs shall keep data, information and documents collected on the basis of the AMLTFL and EU Regulation 2015/847 for a period of 10 years after the termination of the business relationship; the execution of an occasional transaction: (i) of amounting to HRK105 000 (EUR14 000) or more, including linked transactions and (ii) constituting a transfer of funds exceeding EUR1 000; or after access to a safe–deposit box. The exchange offices shall retain all information for 10 years, from the date of collection of CDD information (AMLTFL, Art. 16(1–2), and Art.79(1)).

***Criterion 11.2*** – The specific records that must be retained by REs include: (i) the records obtained through CDD measures; (ii) records on account files; (iii) records on business correspondence; and (iv) records on the results of any analysis undertaken (Art. 79(2(1–4,6–7) and Art.80(1(1–5)). However, the requirement to keep records on results of any analysis undertaken is limited to analysis undertaken in relation to complex and unusual transactions and does not cover other types of analysis undertaken.

***Criterion 11.3*** – FIs are required to maintain notes and records necessary for the identification and monitoring of domestic or cross border transactions (AMLTFL Art.79(2(5)), rather than to allow transactions to be reconstructed as to provide, if necessary, evidence for prosecution of criminal activity.

***Criterion 11.4*** – The AMLTFL (Art.113) provides powers to the AMLO to request information relating to CDD and transaction records. Specifically, Art.113(5) provides for the obligation of REs to submit the required data within the deadline established by the AMLO or within 15 days of the day of the request.

FIs subject to supervision by the CNB are required, upon request, to submit information and reports on all matters and circumstances relevant to supervision (AMLTFL Art.67(6)).

FIs subject to supervision by the CFSSA are required, upon request, to submit information and reports on all matters and circumstances relevant to supervision (Voluntary Pension Funds Law, Art.275(1,4) and Art.278(1), Pension Insurance Companies Law, Art.138(1, 4) and Art.141(1), Insurance Law, Art.203(1, 4) and Art.221(1), Leasing Law, Art.83(1), Factoring Law, Art.72 (1, 4) and Art.77(1), Capital market Law, Art.684(1), OEIFPO Law, Art.346(1,4) and Art.350(1), AIF Law, Art. 232(1, 5) and Art. 236(1).

FIs subject to supervision by the Financial Inspectorate are required, upon request, to submit information and reports on all matters and circumstances relevant to supervision, i.e., data, documentation and information regarding all important circumstances for the performance of an inspection or the implementation of other matters under the Law or other Regulations (Financial Inspectorate Law, Art.10).

The USKOK and other LEAs can obtain CDD and transaction records from FIs, when necessary for investigative purposes under the provisions of the (USKOK Law, Art.49 and CPC, Art. 265(1)).

*Weighting and Conclusion*

FI's are only required to keep records on the results of analyses undertaken in respect of complex and unusual transactions. There is no explicit requirement that the records should be sufficient

to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. **R. 11 is rated LC.**

### *Recommendation 12 – Politically exposed persons*

In the 4th round MER of 2013, Croatia was rated PC with former R.6. There were deficiencies identified in relation to detection of a PEP who is a BO of a customer, and no specific requirement to obtain senior management approval to establish or continue business relationships with PEPs. The requirement to identify the source of wealth of PEPs was only stipulated in the guidelines issued by the FI. The majority of TC deficiencies were addressed, and Croatia was re–rated as LC with former R.6. Some minor concerns remained with the definition of PEP.

***Criterion 12.1*** – The term "politically exposed person" is defined as any natural person who is entrusted with a prominent public function in an EU Member State or non–EU Member State, any natural person who ceased to hold such a prominent public function in at least the past 12 months and includes family members and close associates of PEPs (AMLTFL, Art. (46(2)).

Implementation of EDD measures in relation to PEPs shall be mandatory for at least 12 months from the day one ceases to hold a prominent public function. Nonetheless, REs are still bound to consider the risk posed by persons who have ceased to hold prominent public functions and apply appropriate measures until that person is deemed to not pose a risk in view of his having been a PEP (AMLTFL, Art.46(2), Art.47(3)). Although the FATF Standards prescribe no time frame for the application of EDD measures on PEPs who would have ceased to hold office, the risk–based approach advocated by the AMLTFL is considered to be broadly in line with the requirements.

REs, in addition to the application of CDD, are required to apply additional measures when dealing with PEPs, these include:

*(a) Risk Management Systems*

REs should establish an appropriate risk management system when establishing a business relationship with a customer who is a PEP, or the BO is a PEP (AMLTFL, Art.46(1)). At the same time, the FIs are required to consider among the risk factors related with a customer, whether the latter is a PEP or a BO of a PEP, or whether the customer or the BO of a customer have links with a PEP (CNB and MoF Ordinance, Art.11(2(5–6)), CFSSA Ordinance, Art. 8(5–6)).

*(b) Obtain senior management approval* - FIs should obtain written consent from senior management for the establishment or the continuation of a business relationship with a customer or a BO of a customer who is a PEP (AMLTFL, Art.47(1(1)).

*(b) Establish the source of wealth and funds* - FIs should carry out adequate measures to establish the source of wealth and the source of funds that are involved in the business relationship or transaction in relation to customers or BOs of customers who are PEPs (AMLTFL, Art.47(1(2)).

*(c) Enhanced on–going monitoring* - FIs should conduct enhanced ongoing monitoring of a business relationship with a PEP, which would include business relationships where the customer is a PEP and where the BO of the customer is a PEP (AMLTFL, Art.47(1(3)).

***Criterion 12.2*** – The definition of PEP covers all natural persons entrusted or who have been entrusted with a prominent public function in any EU Member State or a non–EU Member State and also covers natural persons entrusted with a prominent public function within an international organisation (AMLTFL, Art.46(2–3). While Croatia considers that domestic PEPs are covered under the reference to EU–Member States, there is no explicit reference in the legislation.

(a) REs should establish an appropriate risk management system to determine whether the customer or a BO of a customer is a PEP or entrusted with prominent function within international organisations (AMLTFL, Art.46(1)).

(b) The EDD measures explained under criterion 12.1 (b) to (d) are applicable to domestic PEPs, as well as natural persons entrusted with a prominent public function within an international organisation, irrespective of the risk manifested by the respective business relationship (AMLTFL, Art.44(2–3), 47(1)).

***Criterion 12.3*** – The measures set out in c.12.1 and c.12.2 apply to the family members and close associates of all types of PEPs (AMLTFL, Art. Art.44(2–3), 46(1), 47(1)).

***Criterion 12.4*** – REs should undertake reasonable measures to determine whether the beneficiaries of life insurance and other investment–related insurance policy, as well as the BOs of such beneficiaries, are PEPs (AMLTFL, Art.48(1)). These measures must be undertaken, at the latest, at the time of the pay–out or at the time of full or partial assignment of the policy. When REs, on the basis of the risk assessment, identity a high ML/TF risk, they are obliged to carry out at least the following additional actions (over and above the ordinary CDD requirements): (i) inform senior management before the pay–out of insurance policy, and (ii) thoroughly examine the whole business relationship with the policyholder. These additional measures are applicable also in the case of beneficiaries and BOs of beneficiaries who are family members and/or close associates of PEPs (AMLTFL, Art.48(3)). The requirement refers to high–risk scenarios and not higher–risk ones.

However, there are no specific obligations on REs to consider making an STR when a higher risk of ML/TF is identified in connection with a life insurance policy whose beneficiary or BO of the beneficiary is a PEP.

*Weighting and Conclusion*

Most of the requirements for application of additional measures to PEPs are implemented into the legislation. While Croatia considers that domestic PEPs are covered under the reference to EU–Member States, there is no explicit reference in the legislation. There are no specific requirements to consider submitting an STR where higher risks are identified in connection with an insurance policy whose beneficiaries or BOs of its beneficiaries are PEPs. **R. 12 is rated LC.**

### *Recommendation 13 – Correspondent banking*

In the 4th round MER of 2013, Croatia was rated PC with former R.7. There were deficiencies identified with: application of EDD requirements; documenting the AML/CFT responsibilities; lack of clear requirement to obtain senior management approval before establishing new correspondent relationships. Most of the technical deficiencies identified were addressed, and Croatia was re–rated to be LC with R.7. Concerns, however, remained with respect to scope of application of the EDD measures. Since the last MER, Croatia adopted a new AMLTFL in 2018, which was subsequently amended in 2019.

***Criterion 13.1*** – REs should carry out additional measures (to the standard CDD measures) when establishing a correspondent relationship that involves payments carried out with a credit or financial institution having headquarters in a non–EU Member State (AMLTFL, Art.45(1)).

In addition to the AMLTFL, the Ordinances of the CNB, MoF and CFSSA, require that additional measures apply to: (i) non–EU Member States on a risk–sensitive basis; and (ii) EU Member

States, but only where increased risk is present (CNB and MoF Ordinances, Art.33(3), 34, and CFSSA Ordinance, Art.27(3), 28)), which is not in conformity with the FATF Standard.

The additional measures include:

(a) Where applicable to non–EU Member States only: gathering sufficient information on the respondent institution to fully understand the nature of its business operations and determine, from publicly available information, the reputation of the institution and the quality of the business operations supervision, including the information whether the respondent institution has been under investigation for ML/TF (AMLTFL, Art.45(1(1)). This does not include gathering of information on whether the respondent institution has been subject to regulatory action.

Where applicable to non–EU Member States on a risk–sensitive basis, and to EU–Member States with increased risks: collecting information on the respondent to understand its business, reputation, adequacy of supervision (CNB and MoF Ordinances, Art.33(3(1–2)), CFSSA Ordinance, Art.27(3(1–2)). These requirements do not cover a requirement to determine whether the respondent was subject to an ML/TF investigation or regulatory action.

(b) Where applicable to non–EU Member States only: assess the respondent institution's ML/TF prevention system (AMLTFL, Art.45(1(2)).

Where applicable to non–EU Member States on a risk–sensitive basis, and to EU–Member States with increased risks: assess the respondent institution's AML/CFT controls (CNB and MoF Ordinances, Art.33(3(3)), CFSSA Ordinance, Art.27(3(3)).

(c) Where applicable to non–EU Member States only: obtain written consent from senior management prior to the establishment of a business relationship (AMLTFL, Art.45(2)).

Where applicable to non–EU Member States on a risk–sensitive basis, and to EU–Member States with increased risks: obtain approval from senior management before establishing new correspondent relationships (CNB and MoF Ordinances, Art.33(3(4)), CFSSA Ordinance, Art.27(3(4)).

(d) Where applicable to non–EU Member States only: REs should document, rather than understand, the AML/CFT responsibilities pertaining to each institution in the correspondent relationship (AMLTFL, Art.45(1(3)).

Where applicable to non–EU Member States on a risk–sensitive basis, and to EU–Member States with increased risks: document the responsibilities of each institution (CNB and MoF Ordinances, Art.33(3(5)), CFSSA Ordinance, Art.27(3(5)). This does not amount to requiring to clearly understand these responsibilities.

The reference under Art. 28(2) of the CFFSA Ordinance to Art.29 is incorrect. This hampers the application of the EDD measures by investment service providers in relation to an EU/EEA respondent institution for security transactions.

***Criterion 13.2*** – When establishing a correspondent relationship with a non–EU state institution, REs should convince themselves that in relation to payable–through accounts, the respondent institution has: (i) carried out the verification of the customer's identity; (ii) that it continuously carries out due diligence measures of customers that have direct access to the accounts of the correspondent institution and (iii) that, at the request of the correspondent institution, it may provide relevant data regarding the implemented CDD measures (AMLTFL, Art.45(1(4)). These measures are not applicable to EU Member State institutions.

***Criterion 13.3*** – REs are not allowed to establish or to continue a correspondent relationship with a credit or FI should such credit or FI operate as a shell bank, or should it establish correspondent or other business relationships and conduct transactions with shell banks (AMLTFL, Art.45(4)). These measures are not applicable to EU Member State institutions.

In addition, REs are prohibited from establishing or maintaining correspondent relationships with a shell bank; and are obliged to undertake appropriate measures in order to prevent the establishment or continuation of a correspondent relationship with a credit or financial institution which is known to allow a shell bank to use its account (AMLTFL, Art.54(3–4)). These requirements are wider and applicable to both EU member and non–EU member institutions.

*Weighting and Conclusion*

In respect of EU/EEA respondent institutions, additional measures are only applicable where increased risks are identified, and these measures only include those set out under c.13.1(a) (with the exception that there is no requirement to determine whether the respondent institution has been subject to an ML/FT investigation or regulatory action) and c.13.1 (b) and (c). In respect of non–EU/EEA respondents, the requirement to gather information on whether the respondent institution has been subject to regulatory action is only applicable on a risk–sensitive basis (and not in all cases). The additional measures in respect of "payable–through accounts" are only applicable for non–EU and EEA respondent institutions. **R. 13 is rated PC.**

### *Recommendation 14 – Money or value transfer services*

In the 4th round MER of 2013, Croatia was not evaluated against the former SR.VI, having received a C rating in the previous assessment.

***Criterion 14.1*** – In terms of Payment System Law (PSL) (Art.7(1–2)), payment services in Croatia may only be provided by: credit institutions, electronic money institutions and payment institutions, including such types of institutions established in other EU Members States (directly or through branches or agents), and branches of non–EEA credit and electronic money institutions. The provision of payment services by credit and electronic money institutions is governed by the respective laws regulating these institutions (i.e., the Credit Institutions Law and the Electronic Money Act). Credit and E–Money Institutions established in Croatia and branches of institutions based in non–EEA Member States necessitate an authorisation by the CNB to be able to provide payment services in Croatia. Small electronic money institutions are required to be registered with the CNB. Those legal persons who intend to provide payment services as a payment institution require authorisation from the CNB in terms of the PSL (Art.85(1)). Small payment institutions (which may provide a limited number of payment services) are required to be registered (PSL, Art.120(1)). Payment institutions established in other EEA Member States may operate in Croatia subject to the CNB being notified by the host competent authority (Art.140(1)) (as permitted under the applicable EU Directives). Other institutions such as the CNB, the Croatian Bank for Reconstruction which are owned by the Croatian Government, and units of local and regional government may in some instances carry out payment services. HP–Croatian Post (regulated in terms of the Postal Services Act) is also a type of a MVTS operating postal money orders.

Payment services are defined under the PSL (Art.4), and include money remittance defined under Art. 3(1(25). The definition of the term "funds" (Art. 3(1(26)) covers banknotes and coins, electronic money, and scriptural money.

***Criterion 14.2*** – The PSL (Art.80(2) and (3)) require entities to obtain CNB approval for the provision of payment services and subsequently register with the Companies Register before commencing providing payment services. There is no legal provision requiring the CNB, or other authority, to monitor and identify unlicensed activities.

Contraventions of Art.7(2) of the PSL (i.e., unauthorised payment services) are sanctioned in terms of Art.180(1)(8) of the PSL and subject to a fine between HRK 20 000 and HRK 500 000 (EUR5 700–66 500). Art.148(1) of the PSL requires the CNB to notify the State Attorney and other relevant competent authorities where it identifies (through the carrying out of its assigned functions) payment services being provided by unauthorised persons.

***Criterion 14.3*** – Credit Institutions, E–Money Institutions, Payment Institutions, the Croatian Post (when providing postal money orders operations) and the Croatian Bank for Reconstruction and Development, that may provide payment services are all designated as REs (AMLTFL, Art.9) and subject to AML/CFT supervision by the CNB and/or the Financial Inspectorate (AMLTFL, Art.82(1–2)).

***Criterion 14.4*** – In accordance with the PSL (Art. 92(1–2)), a payment institution established in Croatia may provide payment services through one or more agents in Croatia, however, such a payment institution has to first submit an application to the CNB to register such agent/s. This also applies to small payment institutions (PSL, Art. 127). In terms of Art. 93 of the Law the CNB is required to keep a register of authorised/registered payment and small payment institutions, their agents in Croatia and branches in other EU Member States, amongst others. In terms of Art. 93(6–7), the CNB is required to keep the register updated with any changes, while in terms of para. 8 of the same Article, the register has made this register publicly available and accessible on the website of the CNB. Payment institutions from other EU Member States may also provide payment services in Croatia through agents, which have to be entered in the register kept by the competent authority of the home Member State (PSL, Art.140(6)). The PSL does not permit third country payment institutions to operate in Croatia through branches or agents.

***Criterion 14.5*** – When a payment institution (established in Croatia) applies with the CNB to operate through agents in Croatia, it is required to provide a description of the internal control mechanism put in place by such agent/s to comply with the AML/CFT obligations (PSL, Art. 92(3–2)). Furthermore, Guideline 14 of the "*European Banking Authority Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e–money institutions and for the registration of account information service providers*" requires payment institutions to provide information on their internal control mechanisms to comply with AML/CFT obligations including the systems and controls the applicant has or will put in place to ensure that its branches and agents comply with AML/CFT obligations, including in cases where the agent or branch is located in another Member State. This information is required to be provided by payment institutions (established in Croatia) in accordance with the PSL (Art. 85(7)).

The PSL (Art.108(1–2)) stipulates that payment institutions are without any exclusion liable for the acts of their agents. Art.108 (3) furthermore requires that payment institutions carry out on–site and off–site checks of branches and agents at a minimum once a year. Although such checks are understood to include monitoring of compliance with AML/CFT programmes, this is not explicitly stated. In respect of payment institutions providing money remittance Art. 58(4) of the CNB Decision on the assessment procedure of the ML/FT risk and on the manner of applying SDD and EDD explicitly requires money remitters to take reasonable measures to be satisfied that

their agent's AML/CFT controls are appropriate such as by monitoring a sample of the agent's transactions or reviewing the agent's controls.

Agents of EU payment institutions are considered to be REs in their own right subject to the AML/CFT obligations envisaged under the AMLTFL (Art. 9(4)).

*Weighting and Conclusion*

The MVTS are subject to licensing/registration and monitoring, and the payment institution is liable for the agents' actions. However, there are no legal provisions for responsibility for unauthorised operators. **R. 14 is rated LC.**

### *Recommendation 15 – New technologies*

In the 4th round MER of 2013, Croatia was rated C with former R.8. The new R.15 focuses on assessing risks related to the use of new technologies, in general, and imposes a comprehensive set of requirements in relation to virtual asset service providers (VASPs).[78]

***Criterion 15.1*** – ML/TF risk analysis of new products and business practices are captured through the NRA. The latest NRA concluded in 2020 includes an analysis of the ML/FT risks posed by various products and services provided by different sectors of REs such as banks, securities and insurance operators to determine how such product/service risk impacts the overall vulnerability of these sectors. No information was provided on whether there is any legal obligation for the country to assess ML/FT risks associated with new products or services. Although the NRA evaluates various products and services offered by the different sectors, there is no assessment of changing business practices and their ML/FT risk impact.

REs are required to carry out risk assessments to determine and assess the effect that: important changes in business processes and practices, the introduction of new products, externalised activities (i.e., outsourcing of AML/CFT obligations) or delivery channels, and the introduction of new technologies for new and existing products, will have on the ML/TF risk exposure of the RE (AMLTFL, Art.12(6)).

***Criterion 15.2*** – (a)–(b) Before any important changes in business processes and business practice that may have an impact on the measures to be undertaken for the purpose of preventing ML/TF, and when introducing a new product, an externalised activity or a delivery channel, as well as when introducing new technologies for new and existing products, REs shall carry out a risk assessment for the purpose of determining and assessing the way these changes can affect the ML/TF risk exposure, and to apply appropriate measures for the mitigation and efficient management of these risks (AMLTFL, Art.12(6)).

***Criterion 15.3*** – *(a) Identify and assess the ML/FT risks emerging from virtual asset activities and VASPs*

The CFSSA conducted its first assessment of the VASPs sector's ML/TF vulnerabilities which was adopted in May 2021. The assessment was based on 15 VASPs which notified the CFFSA that they were carrying out exchange services between virtual and FIAT currencies or providing custodian wallet services. While this was a basic analysis of the market's economic metrics and an observation of the legislation, broader appreciation of the risks in the sector is yet to be developed. This assessment concluded that ML/TF vulnerabilities are primarily related to a lack of regulatory framework for a range of VASP services.

*(b) Application of risk–based approach in ensuring that ML/FT preventive measures are commensurate to risks identified*

The sector has only been regulated since January 2020. REs are designated as REs and are entitled to adhere to the AML/CFT regulatory framework. Within the CFSSA, a separate unit is setup specialised in engagement with the VASP sector. The CFSSA actively communicates with the VASP sector, detecting new market participants and engaging with them, describing their AML/CFT obligations as a new type of designated RE. Due to the recent nature of the ML/TF vulnerability assessment, Croatia did not yet develop a formal document to design future steps for mitigating respective ML/TF risks.

(c) *VASPs' adherence to criteria 1.10 and 1.11*

Providers, except for the ones engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers are not designated as REs and subject to the AML/CFT obligations. The analysis of c. 1.10 and 1.11 also applies to VASPS, and the deficiencies identified are relevant.

***Criterion 15.4*** – *(a) Licensing or Registration Requirements for VASPs*

There are no licensing or registration requirements for VASPs in Croatia. Natural or legal persons providing exchange services between virtual currencies and fiat currencies and acting as custodian wallet providers are required to notify the CFSSA within 30 days from commencing to provide such services (AMLTFL, Art.9(7)) and if they were already operating before the 1 January 2020, they were bound to notify the CFSSA by the 30 January 2020.

But the obligation to notify the CFSSA does not cover all VASPs envisaged under the FATF Standards. The term "custodian wallet provider" as defined in AMLTFL (Art. 4(50)) is broadly in line with the FATF Standards. The AMLTFL does not cover the full scope of VASPs activities as per the FATF definition. Exchange services between different types of virtual currencies, transfers of virtual assets, and the participation in and the provision of financial services related to an issuer's offer and/or sale of a virtual asset are not subject to AML/CFT obligations.

(b) *Prevent criminals or associates from being involved in VASPs*

There is currently no licensing or registration regime, so consequentially, there are no laws or regulatory measures aimed at preventing criminals or their associates from being involved in VASPs.

***Criterion 15.5*** – For VASPs that are required to notify the CFSSA upon commencing to provide such services, sanctions are applicable in case of failure to do so within the time–frames (AMLTFL, Art.150(1)(65)). The imposed sanctions range between HRK 35 000 – 1 mln. (EUR4 700 – 134 000) where the contravention is committed by a legal person, which may also involve the imposition of a fine (of between HRK 6 000 – 75 000 (EUR 800 – 10 000)) on the members of the management board or on other responsible persons of that legal entity (AMLTFL, Art.150(2)). Where the contravention is committed by a natural person, a fine (of between HRK 15 000 – 450 000 (EUR 2 000 – 60 000)) will be imposed upon such person pursuant to AMLTFL, Art.150(3).

The notification requirements and ensuing infringement sanctions are not applicable to all VASPs covered under the FATF Standards. Furthermore, there is no explicit requirement to require the CFSSA, or other authority, to identify natural or legal persons carrying on VASP activities.

***Criterion 15.6*** – (a) *VASPs are subject to adequate and risk–based AML/CFT supervision*

As noted in c.15.4, not all VASPs envisaged under the FATF Standards are subject to AML/CFT obligations and thus to AML/CFT supervision in Croatia. Furthermore, given this is a new sector under the scope of the AMLTFL, in practice, there has been limited supervision by the CFSSA on the VASPs that notified the supervisor.

*(b) Adequate powers to supervise and monitor VASPs for AML/CFT purposes*

Art.82(5) of the AMLTFL stipulates that for the AML/CFT supervision of VASPs, the laws governing the capital market (i.e., Capital Market Law) and the CFSSA Agency Law also apply. In terms of the Capital Market Law the CFSSA is empowered to carry out direct (on–site) and indirect supervision (off–site) of supervised entities and give recommendations and opinions to supervised entities in order to improve and harmonise their operations and procedures (Art.685(1) and (2)). For the purpose of exercising its supervisory powers, the CFSSA may (i) request the submission of data from supervised entities, employees and other relevant persons (Art.684(1) of the Capital Market Law), (ii) access any document and data in any form, (iii) order the delivery of written statements or take oral written statements and (iv) in case of reasonable suspicion of violations of relevant regulations or upon request of the supervised entity obtain existing records of telephone conversations, electronic communications and other available data traffic records (Capital Market Law Art.684(2)).

The CFSSA may in terms of Art.83(1) of the AMLTFL take a number of measures or actions to ensure compliance by VASPs, including: (i) give written warning and order the removal of irregularities, (ii) file misdemeanour indictments, and (iii) pending the misdemeanour decision temporarily forbid the carrying out of certain business activities or temporarily forbid members of the management board or other responsible persons from exercising managerial duties. Misdemeanour proceedings leading to the imposition of pecuniary fines on VASPs and/or management may be imposed (see c.35.1).

VASPs are not licensed or registered in Croatia, and there is no specific legislation empowering authorities to withdraw or suspend VASPs' ability to carry out business in view of AML/CFT infringements. The CFSSA noted that it can suspend the activities of VASPs as the powers are available under the Capital Market Law, which is one of the governing Laws for supervision. However, the legal applicability of this is questionable given the fact that VASPs are not licensed.

***Criterion 15.7*** – The CFSSA stated that since 2019 seven meetings were held with representatives of VASPs to discuss the existing and potential ML/TF risks pertaining to these activities, and a training event was also held in December 2019, during which a particular session was dedicated to VASPs. The CFSSA has met with representatives of VASPs, and the Association for Blockchain and Cryptocurrencies; and provided guidance on the practical application of AML/CFT obligations. However, given this sector has only been under the scope of AML/CFT supervision since January 2020, not all REs have been risk assessed to determine the level of compliance.

AML/CFT guidance specifically targeting VASPs was not issued. Considering the risks associated with VASPs and virtual assets, the awareness–raising initiatives undertaken have been very limited. In addition to the fact that only a small range of VASP activities are captured by supervision.

***Criterion 15.8*** – (a) *Proportionate and dissuasive sanctions for AML/CFT breaches by VASPs*

The AMLTFL does not make a distinction between types of REs, therefore, all sanctions available under Chapter VII also apply to VASPs. Similarly, deficiencies noted within R.35 will impact

compliance with this criterion. Furthermore, the CFSSA, when determining violations of the provisions of the AMLTFL and by–laws, is authorised to apply the following types of sanctions: written warning; fine; temporary prohibition of certain business activities by the REs or their management; prohibition of carrying out certain duties, activities or tasks by the REs; revocation of licence.

*(b) Sanction applicable on directors and senior management*

Art.150 and 151 of the AMLTFL enable the imposition of sanctions on members of the management board or another responsible person of legal persons.

***Criterion 15.9*** – The preventative measures as set under AMLTFL are equally applicable to VASPs. Therefore, deficiencies of R.10–21 have an impact. As also explained in c.15.4, the AMLTFL does not cover the full scope of VASPs that are envisaged under the FATF Standards. With respect to the limited VASP activities captured:

*(a) CDD threshold for occasional transactions – VASPs*

The occasional transactions designated threshold above which CDD is applicable for VASPs is HRK 105 000 (EUR14 000) – Art.16(1)(2) of the AMLTFL. This is not compliant with the FATF Standards, which require VASPs to apply CDD in the case of lower value occasional transactions (i.e., EUR/USD 1 000 or more).

*(b) Requirements for virtual asset transfers*

There are currently no laws regulating virtual asset transfers in Croatia, and thus no requirements to ensure that virtual asset transfers are accompanied by the accurate originator and beneficiary information as required by the FATF Standards.

***Criterion 15.10*** – In accordance with IRM Law (Art.(10(1)), all natural and legal persons and other entities shall be obliged to act in line with the said Law and to apply the restrictive measures envisaged within it, which would include all VASPs, both those covered under the AMLTFL, as well as others that are envisaged under the FATF Standards but not captured under the AMLTFL.

Moreover, the definition of "assets and other funds" under IRM Law (Art.3) explicitly includes virtual assets as these are defined under the AMLTFL. There are, however, significant deficiencies related to the application of such restrictive measures. See R6 and R7. Furthermore, not all VASP activities as defined by the FATF are captured and subject to sanctions.

***Criterion 15.11*** – The AMLTFL (Art.92) provides the CFSSA with the power to co–operate and exchange information with third country (i.e., non–EU) counterpart competent authorities. However, there are no legal provisions that allow the CFSSA to co–operate and exchange information in relation to the supervision of VASPs with EU counterparts.

FIU–FIU Co–operation is regulated by the AMLTFL (Art.127–137). In particular, AMLTFL (Art.129(1) and 130(1)) expressly enable the AMLO to deliver to foreign FIUs (upon request or spontaneously) data, information and documentation on transactions, funds or persons when there are suspicions of ML/FT. Funds are in terms of AMLTFL (Art.4(40)) defined in a manner that expressly include virtual assets. Deficiencies identified under Rec.37 to 40 apply.

*Weighting and Conclusion*

Whilst the CFSSA carried out a sectorial review that was finalised in May 2021, there are potential limitations to this assessment given there is no licensing or authorisation regime in place for this

sector, hence it is impossible to ascertain the number of firms carrying out this activity. The VASP sector is regulated to some extent, but deficiencies are in place with requirements for registration of the VASPs. Furthermore, the range of VASP activities supervised in Croatia does not extend to the full scope as required under the FATF Standards. Hence, the lack of licensing and limited scope of VASP activities regulated results in major deficiencies. **R. 15 is rated PC.**

### *Recommendation 16 – Wire transfers*

In the 4th round MER of 2013, Croatia was rated LC with former SRVII. The assessment had identified that there was no specific requirement for PSPs of payees to consider the lack of complete originator information as a factor when determining whether a wire transfer was suspicious and thus whether an STR should have been submitted. Since the last assessment a new EU Regulation 2015/847 on information accompanying transfers of funds, was introduced and became directly applicable in all EU Member States on 26 June 2017, repealing EU Regulation No 1781/2006.

FIs carrying wire transfers (hereinafter referred to interchangeably as "transfers of funds") are required to comply with the provisions of EU Regulation 2015/847, which is directly applicable under Croatian Law.

***Criterion 16.1*** – In terms of EU Regulation 2015/847 (Art.4(1–2), all cross–border wire transfers are required to be accompanied by the originator ("payer") and beneficiary ("payee") information as set out under the FATF Standards. Art.4(3) stipulates that when transfers of funds are not made from or to a payment account, the transfer of funds is to be accompanied by a unique transaction identifier which in terms of the definition under Art.3 shall permit the traceability of the transaction. In terms of Art.4(4) and (5), the payment service provider ("PSP") of the payer shall verify the payer's information

***Criterion 16.2*** – EU Regulation 2015/847 (Art.6(1)) provides that in the case of batch file transfers from a single–payer to PSPs of the payees outside of the EU, it is sufficient that the verified information in relation to the payer and the payee is included in the batch file rather than with each individual transaction. Art.6(1) provides that each and every individual transfer within a batch file transfer shall carry the payer's payment account number or the unique transaction identifier.

**Criterion *16.3*** – Art.6(2) of EU Regulation 2015/847 provides for a derogation from the obligations outlined under Art.4(1) (see c.16.1 above) in relation to transfers of funds not exceeding EUR1,000 (single transaction or several linked transactions) where the PSP of the payee is situated outside the EU. Such transfer of funds shall be accompanied by at least the names of the payer and the payee and the payer's and payee's payment account numbers. In the absence of an account, such transfers of funds shall be accompanied by a unique transaction identifier.

***Criterion 16.4*** – Art.6(2) of EU Regulation 2015/847 stipulates that in case of transfer of funds referred to under C.16.3, the information on the payer need not be verified for accuracy by the PSP of the payer unless that PSP has (a) received the funds to be transferred in cash or anonymous e–money; or (b) has reasonable grounds to suspect ML/FT

***Criterion 16.5*** **and** ***16.6*** – In terms of Art.5(1) of the EU Regulation 2015/847 where all PSPs involved in the payment chain are established in the EU (which for the purposes of R.16 would constitute a domestic wire transfer), the transfer of funds shall be accompanied by at least the

payment account number of both the payer and payee or as applicable the unique transaction identifier.

Art.5(2) provides that in such cases the PSP of the payer shall provide, within 3 working days, upon the request of the PSP of the payee or the intermediary PSP the complete information envisaged under C.16.1 (where the transfer of funds exceeds EUR 1,000) or the name of the payer and payee and their payment account numbers or unique transaction identifier (where the transfer of funds does not exceed EUR1,000). Furthermore, Art.14 requires PSPs to respond fully and without delay to enquiries made by competent authorities in relation to information required to be held in terms of EU Regulation 2015/847.

***Criterion 16.7*** – EU Regulation 2015/847 (Art.16) requires the PSP of the payer and payee to retain the information collected on the payer and the payee for a period of 5 years, which may be extended for a further 5 years by national Member States. However, AMLTFL (Art.79(1)) imposes a retention period of 10 years for all data, information and documentation collected on the basis of EU Regulation 2015/847. Personal data collected in terms of EU Regulation 2015/847 shall be deleted upon the expiry of the 10 years retention period (Art.79(4), AMLTFL).

***Criterion 16.8*** – EU Regulation 2015/847 (Art.4(6)) prohibits the PSP of the payer from executing any transfer of funds unless it fully complies with the provisions of Art.4, 5 & 6 reflecting C.16.1–16.6

***Criterion 16.9*** – EU Regulation 2015/847 (Art.10) obliges intermediary PSPs to ensure that all the information received on the payer and the payee accompanying a transfer of funds is retained with the transfer. This is complemented by the provisions of Art.52(1) of the Decision on the measures of payment service providers issued by the CNB (reflecting the technical guidelines issued by the European Supervisory Authorities (ESA) under Art.25 of the EU Regulation), which stipulates that the systems and controls of intermediary PSPs should enable all information on the payer and the payee that accompanies a transfer of funds to be retained with that transfer and transferred to the next PSP in the payment chain.

***Criterion 16.10*** – The criterion is not applicable, because the EU Regulation 2015/847 does not provide for the exemption specified in this criterion regarding technical limitations preventing the appropriate implementation of the requirements on domestic wire transfers.

***Criterion 16.11*** – In terms of the EU Regulation 2015/847 (Art.11(2)), an intermediary PSP has to implement effective procedures, including, where appropriate, ex–post monitoring or real–time monitoring, in order to detect whether the required information on the payer or the payee accompanying a transfer of funds is missing. This is complemented by the Decision on the measures of payment service providers issued by the CNB, which provides more detailed guidance on the detection of transfers of funds with missing information.

***Criterion 16.12*** – The EU Regulation 2015/847 (Art.12(1)) requires intermediary PSPs to establish effective risk–based procedures to determine whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking appropriate follow–up action. This is complemented by the Decision on the measures of payment service providers issued by the CNB, which provides detailed guidance on how transfers of funds with missing information should be managed.

***Criterion 16.13*** – The EU Regulation 2015/847(Art.7(2)) requires PSPs of the payee to implement effective procedures, including, where appropriate, ex–post monitoring or real–time monitoring, in order to identify transfers of funds that lack any of the required information on the

payer or the payee. As stated under c.16.11, the Decision on the measures of payment service providers issued by the CNB provides guidance on the detection of transfers of funds with missing information.

***Criterion 16.14*** – In relation to transfers of funds exceeding EUR 1 000 (whether carried out in a single transaction or several linked transactions), EU Regulation 2015/847 (Art.7(3)) requires the beneficiary's PSP to verify the accuracy of the information on the beneficiary transmitted with the transfer of funds prior to crediting the payee's account or otherwise making the funds available to payee. Art.7(5) moreover states that the PSP of the payee need not verify the payee's information once again upon the receipt of funds if such information is verified as part of the CDD process. The record keeping requirements referred to under c.16.7 apply to the PSP of the payee.

***Criterion 16.15*** – EU Regulation 2015/847 (Art.8(1)) requires the PSP of the payee to implement effective risk–based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow–up action. As stated under c.16.12, the Decision on the measures of payment service providers issued by the CNB provides guidance on the management of transfers of funds with missing information.

***Criterion 16.16*** – EU Regulation 2015/847 (Art.2(1)) stipulates that the provisions of the Regulation apply to transfer of funds (in any currency) sent or received by PSPs (ordering, intermediary and beneficiary) established in the EU. Art.92(3) of the PSA requires PIs to provide a description of the internal control mechanism put in place by agents to evidence AML/CFT obligations.

EU Regulation 2015/847 (Art.2(1)) stipulates that the provisions apply to transfer of funds (in any currency) sent or received by PSPs (ordering, intermediary and beneficiary) established in the EU. The PSA (Art.92(3)) requires PIs to provide a description of the internal control mechanism put in place by agents, to evidence AML/CFT obligations. Furthermore, the PSA (Art.108(1)) assigns responsibility for the agents' actions, to the PI. Hence, although not explicit, the agent will be required to operate in compliance with AMLTFL and the EU Regulation 2015/847.

***Criterion 16.17*** – EU Regulation 2015/847 (Art.9 and 13) require the PSP of the payee and the intermediary PSP to take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds or any related transaction, is suspicious and whether it is to be reported to the FIU.

***Criterion 16.18*** – IRM Law (Art.10(1)) states that natural and legal persons and other entities (which would include PSPs) shall be obliged to act in line with this Law and to ensure direct application of the restrictive measures within their scope of activities. These include the obligations to freeze and/or desist from making funds or assets available to persons or entities designated under UNSCRs 1267 and 1373 and their successor resolutions. There are, however, deficiencies related to the application of such restrictive measures. (See R.6 and R.7).

*Weighting and Conclusion*

Most of the requirements on wire transfer are achieved on the basis of the EU regulatory framework, deficiencies, nevertheless remain in respect to the TFS. **R. 16 is rated LC.**

### *Recommendation 17 – Reliance on third parties*

In the 4th round MER of 2013, Croatia was rated LC on R.9. The main deficiencies were lack of a requirement that the delegating party obtain the necessary information concerning, inter alia, elements of the CDD process, and lack of clear obligation for FIs to take adequate steps to satisfy themselves that data of CDD will be made available from the third party without delay.

***Criterion 17.1*** – The FIs are permitted to rely on third parties to perform elements of CDD (customer identification, BO identification, understanding the nature of the business relationship). Responsibility for CDD remains with the entrusting FI (AMLTFL, Art.38).

(a) The third party is obliged to deliver or make directly available to FI all relevant CDD information immediately (AMLTFL, Art.41(1));

(b) FIs should establish procedures to ensure that they receive respective CDD information from the third party in a timely manner. At the same time, the third party should deliver or make directly available to the FI, without delay, the copy of identification documents and other documentation on the basis of which they have carried out the CDD and have collected the data on the customer (AMLTFL, Art.41(2–3));

(c) There is no requirement for the FI to satisfy itself that the third party is regulated and supervised or monitored and has measures in place to comply with R. 10 and R.11 requirements. Nevertheless, the legislation sets out requirements for the third party (AMLTFL Art. 39 (1)) and establishes punishment for the FI if the entrusted third party does not meet these requirements (AMLTFL, Art. 151(1(2)).

A third party can be: notary public, Financial Agency, HP–Croatia Post Inc., credit institutions, credit unions, investment fund management companies and investment funds, pension companies, investment services firms, and life assurance companies. All of these, except for the Financial Agency, are designated REs under the Croatian legislation (AMLTFL, Art. 9(1–2, 4, 6–8, 18(b), Art. 39(1)). Further on, the legislation sets out requirements that the third party should comply with. This includes: (a) carrying out CDD and record–keeping measures equal to requirements as under the 5th AMLD, (b) being supervised by a competent supervisory authority in equal to requirements as under the 5th AMLD (AMLTFL, Art. 39(1)).

While third parties may have headquarters in foreign jurisdictions that apply the CDD and record–keeping requirement and are supervised in line with the Directive (EU) 2015/849, equal or "equally valuable" provisions, this does not amount to being in line with R. 10 and 11. There are no provisions for the types of entities as mentioned above that are set up outside of Croatia. Any deficiency identified under R.10 (a–c) and R.11 will have an impact here.

***Criterion 17.2*** – There is no obligation for FIs to have regard to information on the level of country risk when determining in which country the third party can be based.

Croatia has determined that the third parties may not be persons having headquarters in a high–risk third country. As an exception, the RE may entrust the third parties having headquarters in a high–risk third country that is a branch or a subsidiary company of the reporting entity from the Member State with the performance of the due diligence, under the condition that it adheres fully to the policies and procedures of the group (AMLTFL, Art.39(2)).

No provisions are set on considering the level of the ML/TF risk that may have a third party from an EU Member State.

***Criterion 17.3*** – The Supervisory authorities may consider that the requirements of the recommendation are met if:

(a) the group applies the CDD measures, rules on record–keeping and programmes against ML/TF in line with the provisions of the AMLTFL or in a way equal or "equally valuable" as the one stated in the Directive (EU)2015/849. Compliance with the AMLTFL does not necessarily amount to compliance with the requirements set out in R.10 to R.12 and R.18.

(b) the effective implementation of the CDD and record keeping requirements at the level of the group is supervised by a competent authority.

(c) No provision to regulate mitigation of higher country risks by group policies is set.

*Weighting and Conclusion*

Croatia implemented some measures related to reliance on third parties, but deficiencies are identified with respect to the requirement for the FI to satisfy itself that the third party is regulated and supervised or monitored and has measures in place to comply with R. 10 and R.11 requirements; obligation for taking into consideration the level of the risk of the country when dealing with the third party based in the EU–Member State; measures applied to FI groups. **R. 17 is rated PC.**

### *Recommendation 18 – Internal controls and foreign branches and subsidiaries*

In the 4th round MER of 2013, Croatia was rated LC on R.15 and PC on R.22. The main deficiencies were related to designation of compliance officers and application of AML/CFT measures related to foreign branches and majority–owned subsidiaries.

***Criterion 18.1*** – FIs are required to implement programmes against ML/TF, which have regard to the ML/TF risks and the size of the business (AMLTFL, Art. 11(2(2)), 13(1–2)). These should include implementation of policies, procedures and controls that contain:

(a) Provisions on position, powers and obligations of the compliance officer within the organisational structure (AMLTFL, Art. 13 (3(3–4)). Appointment of a compliance officer at the management level is, however, dependent on an undefined size and nature of business operations of the RE (AMLTFL, Art. 68(1)).

(b) Provisions on screening procedures of the FIs' employees "if it is appropriate considering the size of the reporting entity and the type, scope and complexity of the reporting entity's business operations" (AMLTFL, Art. 13(3(13)). In addition, there are screening requirements set out for the compliance officers, which are not made dependent on any other similar conditions (AMLTFL, Art. 70).

(c) Provisions on professional training and education for employees of FIs (AMLTFL, Art.13(3(11)). FIs shall conduct regular professional training and education of employees of FIs (AMLTFL, Art.11(2(6)).

(d) Provisions on internal audit of the AML/CFT system –that require for a regular internal audit on the performance of the AML/CFT system, at least once per year should it be appropriate considering the size and nature of their business operations (AMLTFL, Art.13(3,12), 66(7), 67(10), 72). There is no provision that this should be independent. Only banks and the FIs that fall under the supervision of the CFSSA are required to ensure their internal audit function is independent. No requirements for an independent internal audit are set for Credit Unions, PSPs, and E–money issuers or other FIs.

***Criterion 18.2*** – The requirements on group–wide measures do not extend to a model where the FI group is set up and operates within Croatia, with no foreign link. There are no requirements for financial groups to implement group–wide programs against ML/TF. This includes measures set out in c.18.1. The legislative requirements, nevertheless, require FIs, that are part of a group to implement AML/CFT policies and procedures of the group. However, there is no requirement for the FIs to implement group–wide controls.

(a) FIs that belong to a group shall implement the information exchange policy and procedures established within the group for the purposes of AML/CFT prevention (AMLTFL, Art.62(1)). This, however, does not specify whether these requirements would target specifically information exchange for the CDD and ML/TF risk management purposes.

(b) FIs are allowed, unless the AMLO orders differently, to share the following information with a credit or FI from an EU Member State, or its majorly–owned subsidiary or branch from non–EU Member State: information about analysis of a transaction or a customer in relation to which/who there is a suspicion of ML/TF, or that data, information or documentation on a customer or a third person or a transaction was or will be submitted to AMLO (AMLTFL, Art. 74–75). Except for this, there is no regulation on the provision of customer, account and transaction information by branches and subsidiaries for AML/CFT purposes to group–level compliance, audit and or AML/CFT function. Similarly, there is no regulation about receiving such information from group–level functions when relevant and appropriate to risk management.

(c) While there are no specific provisions in respect to safeguards on the confidentiality and use of the information exchange, in particular, to prevent tipping off, AMLTFL, Art.76 requires equivalent data protection measures.

***Criterion 18.3*** – Should the minimum standards for the implementation of AML/CFT measures in non–EU–Member State be less strict than the measures prescribed by the national legislation, FIs should ensure that their branches and subsidiaries adopt and implement appropriate measures that are equal to national legislation, to the extent allowed by the third country (AMLTFL, Art. 64(2)). No equivalent regulation is in place for branches and subsidiaries when situated in the EU Member States.

Should the non–EU–Member State not allow implementation of AML/CFT measures consistent with the home country requirements, FIs should ensure that branches and subsidiaries adopt and implement appropriate additional measures to ensure efficient management of ML/TF risks and should report on that to their respective supervisory authority (AMLTFL, Art. 64(1–3)).

*Weighting and Conclusion*

Croatia has a general regulatory framework on internal controls and group–wide requirements, but there are some deficiencies in this regard. Deficiencies relate to: appointment of an independent audit function to certain FIs but not banks which represent the largest sector; introducing a group–wide AML/CFT programme or instituting group controls; intra–group exchanges of AML/CFT CDD and customer information; coordination between group compliance function; safeguards regarding tipping off and requiring the adoption of AML/CFT measures equivalent to Croatian national requirements by branches/subsidiaries in EU Member States. **R. 18 is rated PC.**

### *Recommendation 19 – Higher–risk countries*

In the 4th round MER of 2013, Croatia was rated LC on R.21. The main deficiencies were related to lack of specific provisions on the application of countermeasures where a country continues not to apply or insufficiently applies the FATF Standards.

***Criterion 19.1*** – FIs are required to apply EDD when establishing a business relationship with a customer linked to a high–risk third country or transaction, including the occasional transaction that involves high–risk third countries (AMLTFL, Art. 44(4), 49(1)). There is no clear requirement to apply EDD proportionate to risks and regard countries called for by the FATF. FIs are required only to take into account the delegated act issued by the European Commission (EC), which identifies high–risk third countries (AMLTFL, Art.49(5)). When identifying countries, the EC is required to take into account relevant evaluations by international organisations in relation to the ML/TF risks posed by individual third countries (5AMLD, Art. 9(4)), this, however, does not suggest that the countries publicly identified by the FATF would always be included into the EC list of high–risk jurisdictions. This EU list excludes EU Countries. EU Regulation (2016/1675) on high–risk third countries with strategic deficiencies (amended in December 2020 by EC regulation 2021/37) only applies to non–EU/EEA states. There is also an element of timeliness, as it requires at least 2 working days when replicating FATF lists. (Methodology for Identifying High–Risk Third Countries under EU Directive 2015/849).

***Criterion 19.2*** – Subject to the deficiency noted in c.19.1, FIs should apply EDD to business relationships and transactions with persons from high–risk jurisdictions. In addition, REs should, in accordance with their own risk assessment of customers when conducting transactions involving high–risk third countries, conduct one or more of the following additional measures of EDD, enhanced reporting mechanisms, introduction of systematic reporting, restriction of business relationships and transactions with high–risk third countries (AMLTFL, Art.49(4)).

In addition, REs should take into account relevant evaluations, assessments or reports drawn up by international organisations and experts responsible for setting standards in the AML/CFT with respect to risks posed by individual third countries (AMLTFL, Art.49(6)). In the application of EDD in Art. 14 (8(1)), REs shall have regard to mutual assessments, and this is not limited to the EU Member States.

The competent supervisory authority, in respect of high–risk third countries identified by the EC delegated act, should be empowered to apply countermeasures related to refusing to establish branches or subsidiaries of FIs from high–risk countries; prohibiting the FIs from establishing branches or subsidiaries in high–risk countries; introducing enhanced supervision or external audit for branches or subsidiaries of FIs located in high–risk countries, including enhances external audit for financial groups in respect to their branches or subsidiaries located in high–risk countries; and order to FIs to reconsider, amend or terminate correspondent relationships with the respondent institution in a high–risk country (AMLTFL, Art. 83a(1)). When applying these measures the supervisory authorities should take into account the high–risk countries called by the EC delegated act (which, not mandatorily, but may include countries publicly identified by the FATF, and may include other countries independently identified by the EC). In addition, the supervisory authorities should also consider relevant evaluations, assessments or reports drawn up by international organisations and experts responsible for setting standards for the prevention of ML and combating against TF in relation to the risks posed by individual third countries (AMLTFL, Art. 83a(2)). Hence, these measures can be applied in both cases: when called by the FATF, and independently from the call by the FATF.

The above–mentioned countermeasures defined for the FIs and supervisory authorities replicate the ones set out by the FATF Standards.

***Criterion 19.3*** – The AMLO and competent supervisory authorities are required to publish the information on higher risk third countries on their website (Art. 49(5)). The MoF and Financial Inspectorate, on the website, publish updated lists of high–risk countries with strategic shortcomings in AML/CFT systems published by both the EU Commission and FATF (in addition provides a link to EU Commission lists and also link to the FATF lists)[223]. Links to both FATF and EU lists are also available on the AMLO, CNB and CFSSA websites[224].

*Weighting and Conclusion*

A provision requiring EDD to be applied to high risk third countries specifically refers to the EC list of high risk third countries. The EU listing mechanism cannot be relied upon as the EU listing is not aligned with FATF, and in any case it does not apply to EU–EEA countries. Nevertheless, FIs are required to apply EDD where there are higher risks which may include higher risk countries not limited to EC countries. The lack of specific reference to publicly named countries by FATF is a deficiency that impacts all three criteria. **R. 19 is rated LC.**

### *Recommendation 20 – Reporting of suspicious transaction*

In the 4th round MER of 2013, Croatia was rated LC with both former R.13 and SRIV. In view of deficiencies with the definition of TF under Croatian Law, the TF reporting obligation did not cover funds that are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance them. Since the last MER, Croatia adopted a new AMLTFL in 2018, which was subsequently amended in 2019.

***Criterion 20.1*** – FIs are required to inform the AMLO, without any delay, when they know, suspect or have reasons to suspect that funds, regardless of their amount, represent the proceeds of criminal activity or are related to terrorist financing (AMLTFL, Art. 56(7)). Where REs cannot report prior to the carrying out of a suspicious transaction (due to the nature of the transaction or for other justifiable reasons –which is not defined), Art. 56(3) allows the reporting to take place after the transaction takes place within not later than the following working day.

The term "criminal activity" is defined as every involvement in the commission of a criminal offence prescribed by CC, and which explicitly includes tax crimes (AMLTFL, Art. 4(21)). ML, as defined for the purposes of the AMLTFL and thus the reporting obligation (AMLTFL, Art. (3(1),(7)) may subsist from the proceeds of any criminal offence. It is explicitly clear that ML would also subsist where the laundered proceeds are generated in a foreign jurisdiction (AMLTFL, Art.3(2)).

The AMLTFL also provides a definition of TF for the purposes of the Law and thus the reporting obligation (AMLTFL, Art. (3(3),(7)), which covers the provision or collection (or attempt thereof) of legal and illegal funds directly or indirectly with the intention or knowledge that they be used,

---

[223] Lista visokorizičnih trećih država_SPNFT.pdf (gov.hr)
[224] AMLO – https://mfin.gov.hr/istaknute–teme/ured–za–sprjecavanje–pranja–novca/143
CFSSA –https://www.hanfa.hr/trziste–osiguranja/sustav–sprjecavanja–pranja–novca–i–financiranja–terorizma/
CNB EC list https://www.hnb.hr/en/core–functions/supervision/prevention–of–money–laundering–and–terrorist–financing/–/asset_publisher/62b7db3014/content/zakonski–okvir
FATF list: https://www.hnb.hr/en/core–functions/supervision/prevention–of–money–laundering–and–terrorist–financing/–/asset_publisher/62b7db3014/content/me–unarodne–institucije–i–grupe–koje–se–bave–problemom–pranja–novca–i–financiranja–terorizma

in full or in part, by a terrorist or terrorist organisation for any purpose (including the commission of terrorist criminal offence) or by persons financing terrorism. This, however, does not explicitly cover the financing of travel for the purposes of perpetrating, planning, preparing for or participating in terrorist acts, or providing or receiving training in terrorism, hence, not fully compliant with R.5, and subsequently this criterion.

***Criterion 20.2*** **–** FIs are required to report suspicious transactions, including attempted transactions, regardless of their amount (AMLTFL, Art.56(5–6)).

### *Weighting and Conclusion*

STR report can be delayed for an undefined "justifiable reason". The definition of TF under the AMLTFL, which is directly relevant and applicable to the reporting obligation under Art. 56 of the AMLTFL, is not fully compliant with R.5 and subsequently hampers the reporting of TF suspicions. **R.20 is rated LC.**

## *Recommendation 21 – Tipping–off and confidentiality*

In the 4th round MER of 2013, Croatia was rated LC with former R.14. The assessment concluded that the protection from liability when submitting STRs was not extended to directors, officials and other natural persons contributing to the direction, management or representation of a reporting entity. Since the last MER, Croatia adopted a new AMLTFL in 2018, which was subsequently amended in 2019.

***Criterion 21.1*** – Provision of data, information, and documents to AMLO does not constitute disclosure of business or professional secrets by FIs and their employees (AMLTFL, Art. 77(1)). Employees of REs are protected from criminal and civil liability for breach of obligation to safeguard the data representing a business and/or professional secrecy when reporting to AMLO STR, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred (AMLTFL, Art.77(3(2)). There is no similar protection offered to directors of FIs.

***Criterion 21.2*** – FIs, directors and their employees are not allowed to reveal to a customer or a third party the following information (amongst others): (i) that the analysis of a transaction or a customer in relation to who/which there is a suspicion is being undertaken by the AMLO or is possible; and (ii) that data, information or documentation on a customer, third person or transaction has been or will be submitted to the AMLO (AMLTFL, Art.74(1(1–2)).

This, however, does not explicitly cover prohibition from disclosing the fact that an STR is being filed with the AMLO. No information was provided on sanctions to be applied to FI, directors, and employees for breach of the requirements under Art. 74.

Where the FI is a part of a group, the provision on tipping–off do not inhibit information sharing under R.18.

### *Weighting and Conclusion*

The protection from liability and ensuing actions are not applicable where disclosures are made by directors of REs. The legislation includes no specific prohibition from disclosing an STR is being filed and there is no sanction for breach of this requirement **R.21 is rated LC.**

### *Recommendation 22 – DNFBPs: Customer due diligence*

In the 4th round MER of 2013, Croatia was rated PC with former R.12. The technical deficiencies mainly cascaded from other R-s. (namely former R.5, 6, 10 & 11). DNFBPs were not required to have in place or take measures to prevent the misuse of technological developments for ML/TF purposes and to address the specific risks associated with non–face to face provision of services. Croatia meanwhile addressed the deficiencies identified in relation to former R.5, which was re–rated to "C" and addressed the majority of technical deficiencies identified with respect to R.6, which was re–rated to "C". No progress was shown in relation to R.10 and 11. Since the last assessment a new AMLTFL was adopted in 2018 and subsequently revised in 2019.

***Criterion 22.1*** – The analysis of R.10 and the respective technical deficiencies identified also apply in relation to DNFBPs. Further findings specific to DNFBPs are outlined hereunder.

(a) *Casinos* –providers of games of chance should conduct CDD when placing bets and taking the gains, including buying or exchange of chips, amounting to HRK 15 000 (EUR 2 000) or more, whether carried out in a single operation or in several transactions that are apparently mutually linked (AMLTFL, Art.16(1(4)). Casinos should also conduct CDD also when there are doubts about the veracity or adequacy of previous obtained CDD data and when there are suspicions of ML/FT (AMLTFL, Art.16(1(4)). The definition of a business relationship explicitly states that the registration of a player with an on–line betting provider creates a business relationship (AMLTFL, Art.4(31)). Thus, on–line casinos are also bound to carry out CDD when establishing a business relationship. The definition of "organisers of games of chance" covers casino games including on–line casinos. The financial transactions that trigger CDD in the case of casinos are thus not limited to gaming transactions that involve only casino chips and tokens (AMLTFL, Art.9(2(16)). Croatia has clarified not to have ship–casinos and also not to have a legislative framework for their licensing.

These obligations are complemented by a requirement for all gaming operators (which includes casinos) to operate and carry out CDD in accordance with the requirements of the AMLTFL (Art.65).

Furthermore, visits to land–based casinos are only permissible to adults who are obliged to identify themselves, and that casino shall determine, check and record the identity of all persons entering the casino by keeping a record containing personal identification data, as well as the date and time of entry into the casino (Law on Games of Chance Art.43(1–2)).

There are no provisions that explicitly oblige casinos to ensure that they are able to link CDD information of specific customers with the transactions they undertake at the casino.

(b) *Real estate agents* –

The authorities did not indicate any legal provisions that specify that real estate agents shall be bound to carry out CDD in respect to both purchasers and vendors of immovable property. However, the Guidelines issued by the Financial Inspectorate specifically to the Real Estate Sector does state that "in accordance with the interpretation of R.22 relating to the non–financial sector (DNFBP), the RE should apply CDD measures in relation to the seller and the buyer."

(c) *Dealers in precious metals and stones* – Legal and natural persons trading in precious metals and stones are considered REs (AMLTFL, Art. 9(2(17(g)). Other traders (besides DPMSs) are considered REs.

DPMSs should identify and verify the identity of customers when they carry out transactions of HRK 15,000 (EUR 2 000) or more (AMLTFL, Art.(16(2)). The fact that the provisions of Art. 15 (stipulating the CDD measures to be applied) and Art. 16(1) (stipulating under which circumstances CDD is to be applied) of the AMLTFL are subject to other provisions and conditions under the AMLTFL (including the provisions of Art. 16(2)) creates legal uncertainty as to whether DPMSs, are required to implement all CDD measures (apart from identifying and verifying the customer).

DPMS should identify customers by collecting specific personal details and referring to identification documents. These requirements are tailored for customers who are natural persons to the exclusion of those who may be legal persons and arrangements. This is mitigated to a certain extent by the fact that in accordance with the Cash Transaction Fiscalisation Law (Art. 28), legal persons may only make payments (for the acquisition of goods or services) in cash up to HRK 5 000(EUR 670) per every receipt (i.e., sale).

Cash transactions above HRK 75 000 (EUR 10 000) are prohibited in Croatia (AMLTFL, Art.55), and hence, c.22.1(c) is not applicable for DPMSs in Croatia.

(d) *Lawyers, notaries, other independent legal professionals and accountants* – Lawyers, law firms, and notaries public are designated REs (AMLTFL, Art.9(2(18b)), and thus required to carry out CDD measures when they participate, whether by acting on behalf of and for their clients in any kind of financial or real estate transaction, or by assisting their clients in the planning or carrying out of the following transactions:

(i) buying and selling of real property or business activities;

(ii) managing of client money, securities or other assets;

(iii) opening and management of bank accounts, saving deposits accounts or securities accounts;

(iv) organisation of contributions necessary for the establishment, operation or management of a company;

(v) establishment, operation or management of trusts, companies, foundations or similar structures.

This corresponds to the list of activities under criterion 22.1(d) and goes beyond by also categorising legal professionals as REs when they Law on behalf and for their clients in any financial or real estate transaction.

Auditors and external Accountants are considered REs when performing accounting services or providing material aid, assistance or advice on tax matters as principal business or professional activity (AMLTFL, Art.9(2(18(a)). These, however, do not cover the activities listed above, as defined by the FATF Standards.

*(e) Trust and Company Service Providers*

TCSPs are designated REs (AMLTFL Art.9(2(17(f)), and consequentially required to apply CDD measures as set out under R.10. when they prepare or carry out transactions for clients in the circumstances identified in the Criterion (AMLTFL, Art.4(36)).

***Criterion 22.2*** – DNFBPs, except for external accountants as described in c. 22.1(d), are subject to record–keeping requirements in the same manner as FIs. The analysis of R.11 and the respective deficiencies are also relevant for DNFBPs.

***Criterion 22.3*** DNFBPs, except for external accountants as described in c. 22.1(d), are subject to PEPs requirements in the same manner as FIs. The analysis of R.12 and the respective deficiencies are also relevant for DNFBPs.

***Criterion 22.4*** – DNFBPs, except for external accountants as described in c. 22.1(d), are subject to requirements in relation to new technologies in the same manner as FIs. The analysis of R.15, and the respective deficiencies are also relevant for DNFBPs.

***Criterion 22.5*** – DNFBPs, except for external accountants as described in c. 22.1(d), are subject to requirements on the reliance on third parties in the same manner as FIs. The analysis of R. 17 and the respective deficiencies are also relevant for DNFBPs.

*Weighting and Conclusion*

The analysis of R.10, 11, 12, 15 and 17 and the respective technical deficiencies identified also apply in relation to DNFBPs, as applicable. No provision obliges casinos to ensure that they are able to link CDD information of specific customers with the transactions they undertake at the casino. The AMLTFL does not establish that external accountants are designated as REs but are not captured under the activities as defined in c.21(d) and consequentially are not bound to carry out CDD measures in line with c.22.1. **R.22 is rated PC.**

### *Recommendation 23 – DNFBPs: Other measures*

In the 4th round MER of 2013, Croatia was rated PC with former R.16. The technical deficiencies underlying this rating cascaded from other recommendations (namely former R. 13, 14, 15 & 21). Since the last assessment, a new AMLTFL was adopted in 2018 and subsequently revised in 2019.

***Criterion 23.1*** – The reporting requirements discussed under Rec. 20 are applicable also to all DNFBPs. However, the external accountants are not fully captured as described in c. 22.1(d). The analysis of R.20 and the respective deficiencies identified also apply in relation to DNFBPs, as applicable.

In addition to the analysis of R.20, there are additional remarks specific for particular DNFBPs outlined below.

The AMLTFL (Art.57(3)) goes beyond the FATF requirements and imposes an additional reporting obligation on lawyers, law firms, notaries public, audit companies, independent auditors, and external accountants to inform the AMLO whenever a customer seeks advice in relation to ML or TF. Such information is required to be provided by not later than the following working day after the advice is sought.

DPMSs are considered an RE when they carry out their business, rather than when they accept cash payments as envisaged under the FATF Standards (since cash transactions above HRK 75 000 (EUR 10 000) are prohibited in Croatia (AMLTFL, Art.55). TCSPs are also considered as an RE when they carry out the activities outlined in c.22.1(e) (AMLTFL, Art.4(36)).

***Criterion 23.2*** – The internal controls requirements analysed under Rec. 18 are applicable to DNFBPs in the same manner as to FI. Findings under 22.1(d) with respect to external accountants apply. The analysis for Rec. 18 and the technical outlined thereunder are applicable to DNFBPs.

***Criterion 23.3*** – The high–risk countries requirements analysed under Rec. 19 are applicable to DNFBPs in the same manner as to FI. Findings under 22.1(d) with respect to external accountants apply. The analysis for R.19 and the deficiencies outlined thereunder are thus applicable to DNFBPs.

***Criterion 23.4*** – The tipping–off and confidentiality requirements analysed under R. 21 are applicable to DNFBPs in the same manner as to FI. Findings under 22.1(d) with respect to external accountants apply. The analysis for R. 21 and the technical deficiencies outlined thereunder are thus applicable to DNFBPs.

*Weighting and Conclusion*

Croatia is partly compliant with R.23. Shortcomings identified under R.18, R.19 and R.21 are equally applicable here. **R. 23 is rated PC**.

### *Recommendation 24 – Transparency and beneficial ownership of legal persons*

In the 4th round MER of 2013, Croatia was rated PC with former R.33. The assessment had highlighted concerns in connection with the misuse of bearer shares for ML purposes, as there was no information available on the number and value of bearer shares still in circulation, no measures were in place to mitigate the risk of bearer shares in circulation and moreover the evaluators were not able to verify the effectiveness of the prohibition on bearer shares introduced in 2008. Since the last assessment, a new AMLTFL was adopted in 2018 and subsequently revised in 2019.

***Criterion 24.1*** – *(a) Identifying and describing the different types, forms and basic features of legal persons*

In Croatia, the following types of legal persons may be set up: Companies (which in terms of Art. 3(3) of the Companies Law include General Partnerships, Limited Liability Companies (LLC) that may take the form of Simple Limited Liability Companies (SLLC), Joint Stock Companies (JSC), Limited Partnerships and Economic Interest Associations), Societas Europea, European Economic Interest Groupings, Institutions, Associations and Foundations. Associations acquire legal personality upon registration in the Register of Associations, which is voluntary (Art.5 and 22(1) of the Law on Associations). Foundations acquire legal personality upon registration in the Register of Foundations. Foundation cannot lawfully carry out activity until it is registered. These types of legal persons, their form and basic characteristics are prescribed under several laws, namely the Companies Law in the case of Companies, the Institutions Law, Law on Associations and Law on Foundations in the case of Institutions, Associations and Foundations, respectively. Societas Europea and European Economic Interest Groupings are regulated by EU legislation, namely EU Regulation No. 2157/2001 and Council Regulation (EEC) No. 2137/85, respectively.

*(b) Process for creation and for obtaining basic and beneficial ownership information*

The process of establishment and registration, and for the obtainment and recording of basic information on different types of legal persons are stipulated under the different laws listed under point (a) above, depending on the type of legal person and the Court Register Law and the Law of the Court Register (for Institutions). The process and requirements posed on legal persons to hold and make available to the BO Register, BO information is set out under the AMLTFL and the Rulebook on BO Register issued by the MoF (see c.24.6). Given that the processes for establishment and the obtainment and recording of basic and BO information are set out in law, these are publicly available.

***Criterion 24.2*** – Croatia possesses a large amount of intelligence and law enforcement information which was not consolidated and analysed in a systemic manner to assess the vulnerabilities of various types of legal persons the extent to which legal persons created or registered in Croatia can or are being misused for ML/TF. The authorities, independently of each

other, demonstrated some understanding of vulnerabilities. While observing that the LLCs and Simple LLCs are the types of legal persons that are most frequently abused, Croatian authorities are reluctant to flag certain types of legal persons as the most vulnerable vehicle for ML, rather are inclined to focus on the schemes and criminal conduct itself (see IO.5).

***Criterion 24.3*** – *Companies and Institutions*

Companies and Institutions acquire the status of a legal entity upon being registered in the Court Register (Art. 4 of the Companies Law and Art. 2 Institutions Law). All Companies, Societe European, European Interest Groupings and Institutions are required to be registered in the Court Register (Law on the Court Register, Art.6). Information that has to be entered in the register for all companies and institutions includes: the name of the entity, the seat and business address, name and surname of persons authorised to represent the entity, the legal organisational form, status changes and the date of adoption of the founding act amongst other information (Law on Court Register, Art.26–32). Companies must submit along with the application for registration in the Court Register the contract of establishment of the entity or articles of association (Companies Law: Art. 70(2) for General Partnerships rendered applicable also for Limited Partnerships by virtue of Art. 132; Art. 394(5) for LLCs; Art. 187(2) for JSCs; and Art. 588(5) for Economic Interest Associations).

Basic Information on Companies (including company name, proof of incorporation, legal form, status, company address, share capital, type of business activities and the list of persons authorised to represent the Company) and Institutions is, in terms of the Law on the Court Register (Art. 4) and the Companies Law (Art. 65), publicly available free of charge through the electronic on–line register https://sudreg.pravosudje.hr/registar/f?p=150:1 The Founding Agreement/Articles of Association are available online if the company was formed online. If not formed online, only the decision on establishment of the company is available for download, but copies of the Founding Company Agreement/Association of the Company/Contract for formation can be requested during office hours.

Since 2019, online company registration has been available using the START system for LLCs and SLLCs. The applications and attachments are prescribed. Documents to be filed with the Court Register are the same. The publicly available information on the criteria for a simplified company can be found in the published Companies Act[225].

*Associations*

Associations are not required to be registered in the Register of Associations administered by the MoJA, and registration is voluntary. However, Associations only acquire legal personality upon registration (Law on Associations, Art.5 and 22(1)). In terms of Art. 23 of the Law on Associations, the application for registration of an association needs to be accompanied by the statute of association (which includes basic information such as name, seat and information on the representation of the association) and other basic information such as the list of founders and the list of persons authorised to represent the association).The majority of basic information on registered associations contained in the Register of Associations is in terms of Art. 24 of the Law on Associations publicly available through the electronic on–line register (https://registri.uprava.hr/#!udruge). The statute forming an association is available on request from the Register of Associations.

[225] https://www.zakon.hr/z/546/Zakon–o–trgova%C4%8Dkim–dru%C5%A1tvima

*Foundations*

Foundations are set up by the formulation of the act of establishment and acquire legal personality and may perform their activities only upon being registered in the Register of Foundations (Law on Foundations, Art. 7(1–2) and 17(8)). In terms of Art. 16(1), Foundations are required to be registered in the Register of Foundations maintained by the competent administrative body of the county or the City of Zagreb. In terms of Art. 15(2), the application for registration of a foundation needs to be accompanied by the act of establishment of the foundation (which in accordance with Art. 7(5) shall include basic information such as the name and seat of the foundation, its purpose, details of the founder/s and information on the property of the foundation. The majority of basic information on registered Foundations is in terms of Art. 24 publicly available through the electronic on–line register (https://registri.uprava.hr/#!zaklade) and includes information on: the name and seat of the foundation, status, date of enrolment, persons authorised to represent the foundation and members of the governing body and the purpose of the foundation amongst other. The charter forming a foundation (Statute of Foundation) is available from the Register of Foundations.

***Criterion 24.4*** – Retention of Basic Information

Not all the types of companies and Institutions are required to maintain the basic information set out under criterion 24.3 themselves. This information is transmitted to the Court Register as explained under criterion 24.3. The Court Register is responsible for maintaining and retention of basic information on a permanent basis[226]. Save that where a company is set up online, and electronic versions of documents are provided, the person submitting the documentation is obliged to retain the originals for 10 years. Likewise, associations and foundations are not bound to keep basic information themselves but are required to transmit such information to the Register of Associations and Foundations respectively for retention on a permanent basis[227].

(a) Companies: Two categories of companies may be set up under Croatian Law: Companies of Persons (i.e., General Partnerships, Limited Partnerships and Economic Interest Associations) and Companies of Capital (LLC and JSC) with the latter type having capital organised in shares (Art. 3(4) of the Company Law).

General Partnerships and Limited Partnerships are not required to keep information on members themselves. Information on the name and address of members is included in the registration application that is to be submitted to the register (Art. 70(1) of the Company Law), which has to be updated whenever there is the entry of new members or termination of membership (Art. 70(3). There is, however, no obligation to notify and keep the registry updated with information on the value of the contribution of each member, nor there is an explicit obligation to notify the registry whenever members cease to be involved in a general partnership or limited partnership.

Economic Interest Associations (EIA) are set up by two or more natural or legal persons in order to facilitate and promote the performance of the economic activities of such members and does not have any share capital (Company Law, Art. 583). Details of the EIA's members have to be submitted to the Court Register for registration of the EIA and any changes thereto are to be

[226] (Article 3(1) of the Law on the Court Register).

[227] (Article 21(1) Ordinance on the Content and Manner of Keeping the Register of Associations of the Republic of Croatia and the Register of foreign Association in the Republic of Croatia and Article 19 Ordinance on the Content and Manner of Keeping the Register of Foundations Register of foreign Foundations in the Republic of Croatia).

notified to the Court Register (Company Law Art. 588(2–3)). The EIA's are not obliged to retain details of their members.

JSCs – In accordance with Art. 226 of the Company Law, registered shares of JSCs shall be entered into the share register of the company indicating the shareholders' name and domicile or the firm name and seat (in the case of legal entities), if the company issued shares without nominal amount and their number, and if it is shares with nominal amounts their number and nominal amount. Commercial court is not obliged to hold details of the shareholders where the shares are in dematerialised form (the information is stored only in the case where only one shareholder holds all the shares of the company). Information on dematerialised shares is held by the Central Depository & Clearing Company Inc. CDCC operates as a central securities depository and a registry of dematerialised securities, where data on issuers, securities, securities accounts, securities holders and other legally required data is kept in the form of electronic records. The top 10 accounts with the most shares (top 10 shareholders) of every security (share)are publicly available by accessing the CDCC website. AMLO, State attorney, Police and the CFSSA for supervisory purposes can access the CDCCS records. The rights and obligations of shares are only considered to pertain to the person who is registered as their shareholder in the company's shareholder register (Companies Law Art. 226(2)). There is, however, no obligation to retain information on the categories of shares, and there is no explicit obligation for JSCs or their management board to retain the register of shares for any period of time, and no specific obligation to retain it within Croatia and to notify the Court Register as to where such information is held.

LLCs – Art. 410 of the Company Law requires the management board to keep a book of the company's business shares (share register) which shall include: the name and surname, residential address or seat (if the company member is a legal entity) of each member of the company, business shares that he/she has taken over and what he/she has paid on that basis and any additional actions that he/she is obliged to fulfil towards the company (all liabilities arising from the business share and the number of votes he/she has in making decisions. Encumbrances and divisions of business shares and all other changes are also entered in the book. Any person who can prove that he or she has a legal interest in doing so has the right to review the book of business shares of the company during working hours. Art. 411(1) stipulates that only those members entered in the book of business shares and notified to the Commercial Court are recognised as members of the company. There is no specific obligation to retain the book of the company's business shares within Croatia and to notify the Court Register as to where such information is held.

(b) Associations, Foundations and Institutions – An association is obliged to keep a list of its members. The list of members must contain information on personal name, personal identification number (OIB), date of birth, date of joining the association, membership category, if determined by the statute of the association and date of termination of membership in the association (Art. 12(3) and (4) of the Law on Associations). There is no explicit obligation to retain such information within Croatia at a location that is notified to the Register of Associations. A foundation is an asset holding vehicle intended to serve the realisation of a public benefit or a charitable purpose and is a non–profit legal entity without members (Art. 2 of the Law on Foundations). Institutions are set up by founders that may be domestic or foreign natural or legal persons. A public institution may be set up by the Republic of Croatia, local or regional government or another legal or natural person (where permitted by special law) for the permanent performance of activities of public interest as regulated by law (Art. 1 and 7 of the

Institutions Law). Institutions do not have any members or shareholders but the founders who are responsible for the obligations of the Institution, and if there are several founders, the mutual rights and obligations of the founders are regulated by the contract establishing the Institution. The contract of establishment may not exclude or limit the liability of the founders for the obligations of the institution. The act (including where more than one founder the contract) of establishment includes the name and residence of the founder(s) and is filed with the Court. Information regarding the founder has to be entered into the Court register, and changes have to be entered in the Court register.

***Criterion 24.5*** – In most cases, the Companies Law is silent regarding the timeframes for updating information, but Art. 9(2) of the Law on Court Register requires an application for changes in recorded information to be submitted within 15 days from when the precondition for application subsists (i.e., when the change materialises). Companies – In the case of general partnerships and limited partnerships, Art. 70(3) of the Company Law (which is rendered applicable for limited partnerships via Art. 132) specifies that changes in the articles of association, company name and registered office, entry of a new member into the company, termination of membership in the company and changes to the representatives of the company or partnership shall be entered in the court register. This does not, however, tantamount to an explicit obligation to notify the Registry of such changes.

JSC and LLC – Amendments to the JSC's statute or LLC Articles of Association become valid once they are entered into the register (Company Law Art. 303(3) and 454(2)). Art. 303(1) and 456(1) specify the manner in which changes to the statute or articles of association have to be notified to the Court Register, requiring the submission of an application accompanied by a notarised full text of the statute/articles. The notary public must confirm the accuracy of the full text of the revised statute/articles submitted together with the application, attesting that it contains all amendments agreed to by the company and that the unchanged sections correspond to the version of the statute/articles held by the Court Register. These provisions, however, do not explicitly oblige a JSC or LLC to notify the registry with changes to the statute/articles. The statute, moreover, does not include information on the directors of the company, nor does it indicate the company's basic regulating powers. In the case of LLCs, changes to company directors are required to be notified without delay in terms of Art. 425(1) of the Company Law. Without delay is not defined, so the timeframe specified in Art. 9 (2) of the Law on Court register would apply. No information was provided as to how changes to the [directors] management board members of the LLCs or to the JSC's and LLC's basic regulating powers are notified to the register. Changes to the [directors] management of JSCs have to be made in accordance with Art. 245(a) of the Company Law.

With regards to changes in shareholders of JSCs, Art. 226(3) of the Company Law states that when a share is transferred, the register of shares shall be updated upon request accompanied by proof of share transfer. The company may, in terms of the same article, request shareholders, who are obliged to inform it, whether shares held are owned by them. Intermediaries (who may be holding shares on behalf of shareholders) are also obliged to provide the company with all the necessary information for keeping the stock register. The fact that there is no time frame within which share transfers are to be notified to the Company and that the update of the register of shares is totally dependent on the shareholder making a request undermines the company's ability to retain accurate and updated information on its shareholders. This is to a certain extent mitigated since shareholding rights are only recognised upon entry in the register (see c.24.4).

LLCs are required to keep the book of business shares updated with any changes, and the management board is obliged to inform the Court Registrar on any change to the company members or their business shares without delay (not defined see para. 0 above) by submitting an updated list of company members, signed by the members of the management board (Art. 410(2) of the Company Law). Similarly to JSCs, the updating of the business register is occasioned by a request of an interested party (e.g., shareholder), or if the company becomes knowledgeable of any changes, however, there is no explicit obligation for shareholders to notify the company of such changes. This undermines the company's ability to retain accurate and updated information on its shareholders. To a certain extent, this deficiency is mitigated since shareholding rights are only recognised upon entry into the register (see c.24.4).

Economic Interest Associations – Art. 588(3) of the Law on Companies indicates that changes to basic information, as well as members of the association should be notified to the Court Registrar, even though the wording of the law could benefit from more clarity. As explained earlier, Art. 9(2) of the Law on Court Register requires an application for notification of changes to be made within 15 days.

Institutions like companies have their basic information registered in the Court Register, and the Law of the Court Register requires information to be updated (Art. 24 and 33).

Save for where a notary is required to verify documents, no information was provided on procedures of the Court Register to test/verify the accuracy of the basic information held on the Court register in relation to the formation of legal persons or after the information has been changed. Nor was any information provided on sanctions imposed for filing inaccurate basic information.

Associations and Foundations: Persons responsible for the representation of associations and foundations are bound to notify the Registrar of Associations/Foundations when there are changes to basic information or the statute of the association/foundation and submit all necessary evidence (Art. 27(1) of the Law on Associations & Art. 19(1) of the Law on Foundations). In the case of Associations, Art. 27(3) requires that such changes be notified to the Registrar within 60 days, while Art. 27(5) stipulates that such changes become legally applicable upon entry in the register. There are no time–frames for the notification of changes in the case of foundations.

As explained under criterion 24.4, associations are obliged to keep a list of members, which should include the date when members join and leave the association. This implies that the list of members is to be kept updated, although there is no explicit obligation to do so. Foundations do not have members (see criterion 24.4).

A request for change accompanied by necessary evidence in relation to an Association/Foundation is submitted to a public servant who has to determine the facts and can reject the application or can seek further clarifications. These clarifications are limited factual accuracy, no information was provided on any checks undertaken, no qualifications in law are prescribed for these civil servants, but normally they will have competed in tertiary education with a law degree. Reasons for rejecting the application for associations are prescribed in Art. 27 of the Law of Associations and Art. 19 of the Law of Foundations. If the legal conditions are met, a decision on entry is made, and data is entered into the Register of Associations.

***Criterion 24.6*** – Croatia relies on a number of mechanisms to ensure that BO information on companies and other legal persons set up under Croatian law is available.

(i) Legal persons (Companies, Branches of Foreign Companies, Associations, Foundations and Institutions) established in the territory of Croatia are obliged in terms of AMLTFL (Art. 33(1)) to have appropriate, accurate and updated information on their BOs (name and surname, country of residence, date of birth, identification number or information on identification document, citizenship and information on the nature and extent of BO), and on the ownership structure. Companies are also required to have data on the percentage of shares, stakes, voting rights, any other means of control over the legal entity is exercised or any other form of participation in the ownership of the company.

AMLTFL (Art.33(6)) puts an obligation on BOs of these legal persons to provide the information outlined under para. 1(a) to the management board or legal representatives of the legal person. In terms of AMLTFL (Art. 33(4)) such legal persons are obliged to input data on their BOs in the BO Register that is maintained by the Financial Agency on behalf of the AMLO. The Rulebook on BO Register issued by the MoF prescribes the manner and time–frames for inputting BO information. In accordance with the Rulebook (Art. 14), legal persons that were already in existence upon the setting up of the register of BOs were required to input in the register information about their BOs by 31 December 2019. Legal persons established after 1 December 2019 are obliged to enter the BO data in the Register but not later than 30 days from the establishment date of the legal person.

Moreover, in populating the BO register, the Financial Agency is granted access to the various registries that hold information on various types of legal persons, including the Court Register and the Registers of Associations and Foundations, and also access to information on such legal persons held by the TA.

As stipulated under AMLTFL (Art. 34(1)) of the (and complemented by more detailed provisions under the Rulebook), the register of BOs is accessible to the AMLO, supervisors and other services within the MoF (i.e., Financial Inspectorate, TA and CA), the MoI (which includes the Police, PNUSKOK) the CNB, CFSSA, the SAO, the SIA, and other state authorities and various government ministries. The register is also accessible to REs (subject to varied access methods and levels), and the public has access to limited data that is available free of charge online[228] (ii) As mentioned under c.10.5 and c.10.10 REs are required to identify and verify the identity of BOs of customers that are legal persons and are moreover required to retain such information for 10 years after the termination of the business relationship or the carrying out of an occasional transaction (see c. 11.2).

Such records are accessible to the AMLO, which may order the delivery of BO information within a stipulated time and not later than 15 days.

Art. 67(6) of the AMLTFL and sector–specific laws include requirements binding REs to provide all documentation, reports and information that is necessary for supervisory purposes. Thus, the CNB, Financial Inspectorate, the CFSSA and TA can access BO information via supervised REs when conducting supervisory actions.

Art. 36(4) of AMLTFL enables the TA to obtain BO information from legal persons directly.

Law enforcement authorities may access CDD information (including BO information) held by REs upon court order, in line with the CPC provisions. Mechanisms exist for the LEAs, where there

[228] https://rsv.fina.hr/RSV–OnLineUnos–web/login

are reasonable grounds to believe a criminal offence has been committed, to obtain BO directly from legal persons.

Information on listed companies is publicly available on the Zagreb Stock Exchange, which imposes rules on shareholding as set out in the listing rules[229].

As discussed under c. 10.10 (BO Definition), certain shortcomings related to the manner in which the "BO" concept is defined under the AMLTFL may undermine the accuracy and extent of BO information that is available through the above mechanisms.

***Criterion 24.7*** – There are various measures and mechanisms to ensure the retention of accurate and up–to–date BO information of legal persons set up in Croatia, and additional measures regarding interaction between databases are in the pipeline.

Companies and other legal persons (Companies, Branches of Foreign Companies, Associations, Foundations and Institutions) are bound to have appropriate, accurate and updated information on their BOs (AMLTFL, Art. 33(1)). The Rulebook on BO Registry (Art. 15(1)) requires legal persons to provide to the registry updated information on their BOs, whenever there is a change in BOs. Such updated information has to be provided to the registry within 30 days from when a change occurs.

The AMLTFL and the Rulebook provides for specific supervisory mechanisms to ensure that accurate BO information is being provided by legal persons and in a timely manner. The Rulebook (Art.18) provides that the Financial Agency shall perform supervision based on verification of data held in the Register to determine whether the BO information that is required to be provided by legal persons under the Law and Rulebook has been provided and has been provided within the timeframes specified. Moreover, the TA is in terms of the AMLTFL (Art. 36) and the Rulebook (Art. 19) tasked to supervise legal persons that are obliged to provide BO information to the register and to determine whether they have accurate and complete data on their BOs and whether they have registered accurate and complete data BO information in the prescribed manner and within the specified deadlines.

No information was provided on procedures of FINA to test/verify BO information provided within the required timeframes. No information is provided on procedures of the TA to test/verify the accuracy of the BO information in the BO Register or after the information has been changed. As indicated, the TA checks BO information when it conducts a tax audit/investigation. No Misdemeanours have been issued relating to the verification of the accuracy and timeliness of data entry in the BO Register. There is currently a moratorium on the application of misdemeanour proceedings for failing to populate the BO Register or update it, set for an undefined period. Hence, there is not mechanism to enforce the supervisory mechanism and ensure that the BO Database is populated with accurate and up–to–date information.

The AMLTFL (Art.35.a) provides for a mechanism for the reporting of noted discrepancies on BO information. RE and other competent authorities are bound to inform the AMLO when they note that BO information that they hold on a legal person does not correspond with the BO information held in the Register. The verification should be performed on the basis of materiality and risk, hence, in the absence of a risk–event this may result in a RE, taking a number of years to update BO information on an existing customer. When received, the AMLO is then required to notify the

[229] Listing Rules and Regulations (zse.hr)

Financial Agency and the TA so that they take into account these flagged discrepancies when supervising legal persons for adherence to their BO transparency requirements).

(iv) REs establishing business relationships with legal persons set up in Croatia are required to take measures to ensure that CDD information (including BO information) is kept up to date. Issues with timeliness of verification of the BO information, as described above, apply also here. REs are supervised for the implementation of their AML/CFT obligations by the various sectorial supervisory authorities.

***Criterion 24.8*** – As set out under c.24.6 legal persons established in the territory of Croatia are obliged to have appropriate, accurate and updated BO information, (Art. 33 (3) to (5) AMLTFL) are obliged to input such information in the BO Register, and are also obliged to update the Register whenever there are changes to the BOs (see c.24.7).

However, there is no requirement under Croatian Law for the members of the management board or other responsible persons (in the case of other types of legal persons besides Companies) to be resident in Croatia and be accountable to competent authorities for it.

DNFBPs are required to provide BO information of legal persons to AMLO for performing its operational and strategic analysis (AMLTFL, Art.113(1–4)). However, there is no specific legal provision requiring that a DNFBP be authorised by the company, and accountable to authorities, for providing all basic and BO information, as well as providing further assistance.

***Criterion 24.9*** – *Retention of Basic Information*

In terms of Art. 3(1) of the Law on the Court Register, all basic information on Companies and Institutions that is required to be registered (see c.24.3) shall be kept permanently by the Commercial Courts. Likewise, all basic information on Associations and Foundations that is required to be transmitted to the Register of Associations and Foundations is held on a permanent basis (see c.24.3).

General Partnerships, Limited Partnerships and Economic Interest Associations are not required to keep information on members themselves (see c.24.4.). This information is kept by the Commercial Court (Court Register) and hence required to be kept permanently. In the case of JSCs and LLCs, shares and shareholder information is required to be entered into share registers, although there is no explicit obligation on JSCs and LLCs to keep share registers for any period of time – see c.24.4. Upon the dissolution of a JSC or an LLC, the liquidator shall pass on the company's accounts and documents, including share/shareholder information to the Croatian Chamber of Commerce for safe–keeping (Art. 382(4) and 472f of the Law on Companies). No timeframe is given for the period during which the information should be retained.

Associations are required to maintain a list of members (Art 12 (3)). No timeframe for retention of this information is specified.

*Retention of Beneficial Ownership Information*

BO Information of legal persons set up in Croatia that is registered in the BO Register shall be kept permanently registered (AMLTFL, Art. 32(4) and the Rulebook Art. 10(4)), irrespective of whether the legal person ceases to exist.

REs are required to retain basic and BO information of the customer that are legal persons for 10 years after the termination of the business relationship or the carrying out of an occasional transaction (see c. 11.2).

***Criterion 24.10*** – Basic information on legal persons held in the respective registers for Companies, Institutions, Foundations and Associations is publicly available through the various electronic registers and by request where not held electronically (see c. 24.3).

As explained under c. 24.6 the BO Register is accessible to the AMLO, supervisors and other services within the MoF (i.e., Financial Inspectorate, TA and CA), the MoI (which includes the Police, PNUSKOK), the CNB, CFSSA, the SAO, the SIA and other state authorities and various government ministries.

Moreover, CDD records (including basic and BO information of customers that are legal persons) retained by REs are accessible to the AMLO, although within 15 days from making a request. Generic requirements under Art. 67(6) of the AMLTFL and sector–specific laws bind REs to provide to supervisors all documentation, reports and information. This is interpreted to also include CDD and BO information of their clients, although not in an explicit manner.

Photographic ID documents are not held in the BO Register. A photographic ID document is required for the verification of the identity of the person authorised to enter data into the BO Register.

***Criterion 24.11*** - As set out under c. 24.4. only JSCs and LLCs are considered to be Capital Companies (Art. 3(4) of the Company Law) having capital organised in shares. Hence only these two types of legal persons were assessed for compliance with this criterion.

From the 1 April 2008, JSCs in Croatia are no longer allowed to issue shares in bearer form. Art. 170 and 171(2) of the Law on Companies stipulate that all shares issued by JSCs must include the name and surname of the person for whom the share has been issued, which component is to be included in the share document. Croatian Authorities have indicated that no specific measures were taken to change bearer shares (issued pre–2008) into registered shares. According to data from the central securities depository, 5 JSCs issued bearer shares out of a total of 690 JSCs. Those 5 companies have issued a total of 330.832.874 shares, 66.023 of which are bearer shares. No data is available on how many of these have been converted into registered shares. Under the current legislative provisions, bearer shares cannot be transferred, exercise any rights attached to them, such as the right to vote or being traded without BO being ascertained.

LLCs legislation has never permitted the issuance of bearer shares.

***Criterion 24.12*** – No information was provided to indicate that the concepts of nominee shareholders or nominee directors are prohibited by law in Croatia, or that criterion 24.12 (a), (b) or (c) are met. In terms of nominee shareholder arrangements, an example was given in the 2020 NRA, in relation to tax evasion, of an "… account held by a Croatian company controlled by the offender but formally owned by a person subsequently to be homeless, a person with special needs or persons with dual citizenship…".

The Companies Law (Art.148) permits secret societies, which are a form of secret partnerships where a secret member invests in an entrepreneur's business and may benefit from eventual profits of the business. Art.148(5) provides if a notary is involved in drawing up the secret society contract, they have to submit a copy of the TA, if there is no notary, then the entrepreneur has within 15 days of the conclusion of the secret society contract to submit a copy to the TA. Art. 153 indicates "the death of a secret member does not lead to the dissolution of the society". There is no requirement to update the TA as to a change in secret member or other BO of the interest created by the secret society contract unless the secret society contract is changed. Information regarding the beneficiary of a secret society contract would only be included in the BO register if

they had a controlling interest. A secret society agreement directly with a JSCs or LLCs is a business of agreement that has to be registered with the Court under the Companies Law (Art.480), contracts for a partial share of profits with employees, members of the supervisory or management board or executive directors do not have to be registered.

***Criterion 24.13*** – Under the Company Law (Art.630) sanctions may be imposed on all types of companies for failure to enter the required data in the Court Register and for failure to notify the Court Register with the termination of the company or the expulsion or withdrawal of a member. This same article also lays down sanctions:

*(i)* for JSCs that: fail to enter registered shares in the register of shares and fail to report to the Court register: changes in the composition of the supervisory or management board and changes to the statute;

*(ii)* for LLCs that do not keep a book of business shares or do not keep it properly, that do not notify the Court Register with: changes to the book of business shares in time or provide incorrect notifications, changes to the composition of the management board and changes to the articles of association.

A fine of up to HRK 50 000 (EUR 6 700) may be imposed on the Company for the above–mentioned breaches, while company responsible persons may be fined up to the amount of HRK 7 000 (EUR934) for these same violations or a fine up to the amount of HRK 50 000 (EUR 6 700) if the violations are considered serious and have been committed in order to acquire illegal property gain.

Art. 631, on the other hand lays down sanctions for persons who do not provide to a JSC information on their shareholding or provide incorrect, incomplete or untimely information. For such breaches, a fine of up to HRK 7 000 (EUR 934) or up to HRK 50 000 (EUR 6 700) in the case of serious breaches committed in order to acquire illegal property gain may be imposed.

The Associations Law and the Foundations Law do not apportion liability or prescribe sanctions for violations, although supervisory action can be taken for failure to comply with the requirements, which may result in a fine being imposed if there is failure to eliminate deficiencies and irregularities (General Administrative Procedure Law, Art.139).

The AMLTFL (Art. 153(4–9) prescribe sanctions for legal persons that do not adhere to their obligations to hold accurate and updated BO information and to provide such information to the register of BOs in a timely manner. Fines ranging from HRK 5 000 (EUR 670) to HRK 350 000 (EUR 47 000) may be imposed on legal persons, while fines ranging between HRK 5 000 to HRK 75 000 (EUR 670 to 10 000) may be imposed on the members of the management board or responsible persons of legal persons. For the most severe types of contraventions (and where proceeds are gained or damage caused), the maximum fine on the legal person may increase up to twice the amount of benefit derived from the contravention or HRK 750 000 (EUR 100 000), while the maximum fine on the members of the management board or responsible persons of such a legal person may increase up to HRK 100 000 (EUR 13 000).

Sanctions are available under the AMLTFL for REs, members of the management board and responsible persons of such REs for failure to carry out their AML/CFT obligations under the AMLTFL, including the identification and verification of BOs, the retention of CDD information (including BO information) and the provision of information to the AMLO upon request (see R.35) and provision of CDD information to the relevant competent supervisory authority.

***Criterion 24.14*** – As set out under c. 24.3 the respective official registers (Court Register, Register of Associations, Register of Foundations), which hold basic and shareholder information (names and other personal details of shareholders) of companies and other legal persons, are publicly available.

With regards to BO information that is held in the BO Register, the AMLTFL (Art. 34(2) clearly stipulates that the AMLO, supervisors and other services within the MoF (i.e., Financial Inspectorate, TA and CA), the CNB, CFSSA, the SAO, the SIA, the MoI (which includes the Police) and other state authorities (among others) shall have timely and unrestricted access to the register to perform the tasks within their competence (including that of exchanging information with foreign counterparts). Art. 34 further states that these competent authorities are required to transmit BO information held in the Register to their foreign counterparts in other EU Member States when requested.

Analysis and deficiencies identified in R.37–40 are relevant here.

***Criterion 24.15*** – The AMLO and Police don't monitor and keep ratings on the quality and usefulness of basic and BO information received from foreign FIUs. However, the AMLO and Police indicated that they would be able to give feedback on the quality of information provided when requested by the foreign counterparts. Other competent authorities have not explained how they monitor the quality of assistance received from counterparts in foreign jurisdictions.

### *Weighting and Conclusion*

Information on how to set up types of legal persons in Croatia is publicly available online. Online registers provide access to basic and BO information. While no formal risk assessment of each type of legal person has been conducted in the NRA typologies, trends and case studies have been provided. There is a small gap (8.2% as of 1 May 2021) in the BO Register information. General Partnerships and limited partnerships are not required to keep details of members. There is a lack of verification/testing of the accuracy of basic and BO information. There is no requirement for the members of the management board or other responsible persons to be resident in Croatia, which would hinder co–operation with the company from make basic and BO data available promptly. There is evidence of the existence of nominee shareholders/directors but no mechanisms to deal with them. **R.24 is rated PC.**

## *Recommendation 25 – Transparency and beneficial ownership of legal arrangements*

In the 4th round MER of 2013, former R. 34 was not considered applicable to Croatia since there were no provisions under Croatian legislation that permit the formation of trusts. Croatian Law still does not provide for the creation of trusts or similar legal arrangements. This is also confirmed by the "*List of trusts and similar legal arrangements governed under the law of the Member States – (2019/C 360/05)"* published by the EU Commission and based on notifications made by EU Member States which were required in terms of Art. 31(10) of the 4th EU Directive to indicate the trusts and similar legal arrangements that could be set up under their national laws. Although trusts and similar legal arrangements may not be set up under Croatian law, there is nothing preventing Croatian residents from setting up trusts in foreign jurisdictions, while trusts and similar legal arrangements created under foreign laws are not precluded from conducting activities and entering into business relationships with or carrying out transactions through REs in Croatia. Moreover, legal and natural persons in Croatia may also act as trustees and provide other trust–related services. Under the revised FATF 2012 Standards, R.25 includes a number of elements that are applicable to all jurisdictions and not only those which provide for the creation

of trusts under their laws. Furthermore, since the last evaluation, a new AMLTFL which provides for new BO transparency requirements was adopted in 2018 and subsequently revised in 2019.

***Criterion 25.1*** – Trusts and similar legal arrangements may not be set up under Croatian Law. Hence, requirements under sub–criterion (a) and (b) are not applicable.

(c) Trusts and similar legal arrangements set up under foreign laws may still carry out financial and other activities in Croatia. The trustees are recognised as REs and are required to conduct and retain CDD information for 10 years after the termination of the business relationship or the carrying out of an occasional transaction (see c. 11.2).

The same approach applies to lawyers, law firms and notaries public (and not the accountants) (AMLTFL, Art.9(2(18(b)), within the scope of being RE – and the record keeping requirements – when they are establishing, operating or managing trusts. See c.10.7 and R.22.1 on keeping records up to date.

***Criterion 25.2*** – There are various measures and mechanisms to ensure the retention of accurate and up–to–date BO information on foreign trusts or similar legal arrangements that are serviced by Croatian REs, or which carry out certain activities in Croatia.

(i) Trustees of foreign trusts (or persons in equivalent provisions in the case of similar legal arrangements), in the circumstances outlined in c. 25.1, are bound to have appropriate, accurate and updated information on the BOs of such foreign trusts (Art. 33 paragraph 3 and Art. 7 of the Rulebook on BO Register). Art. 15 paragraph 1 of the Rulebook requires trustees to provide to the registry updated information when there are changes to the BO information of foreign trusts. Such updates have to be provided to the registry within 30 days from when a change occurs. No evidence of any checks conducted regarding compliance with this requirement was provided.

(ii) The AMLTFL and the Rulebook provide for specific supervisory mechanisms to ensure that accurate BO information is being provided by trustees (and similar persons in relation to other legal arrangements) and in a timely manner. See the explanations provided under c.24.7(ii), since such supervisory mechanisms apply to both legal persons and trustees (in relation to BO information of foreign trusts). It is, however, questionable how such supervision may be exercised, in practice, especially in relation to trustees (or similar function holders) that are not resident or established in Croatia).

(iii) The AMLTFL (Art.35.a) provides for a mechanism for the reporting of noted discrepancies on BO information of foreign trusts or legal arrangements. See the explanations provided under c.24.7(iii), since the discrepancy reporting arrangements are likewise applicable to BO information of foreign trusts and legal arrangements.

(iv) REs establishing business relationships with foreign trusts are required to take measures to ensure that CDD information (including BO information) is kept up to date, although certain deficiencies were noted with the requirement to keep CDD data updated (see c. 10.7). Moreover, the technical deficiencies in relation to the obligations to identify and verify foreign trusts and similar legal arrangements and their BOs highlighted under c.10.9 and c.10.11, affect the adequacy and accuracy of BO information on such foreign trusts available through REs and consequentially the BO Register. REs are supervised for the implementation of their AML/CFT obligations by the various sectorial supervisory authorities.

***Criterion 25.3*** – In accordance with the AMLTFL (Art. 30(3–4)), trustees and persons performing equivalent functions in the case of similar legal arrangements shall, when establishing a business relationship or carrying out an occasional transaction with a reporting entity, disclose to the

respective reporting entity, in a timely manner, the fact that they are acting as trustees (or similar function) of a trust/legal arrangement, and shall also provide information on the identity of the persons listed under AMLTFL (Art. 31(1)) i.e., the settlor(s), any other trustee(s), protector(s), beneficiaries or class of beneficiaries, similar functions in the case of other legal arrangements and any other persons controlling the trust through other means.

***Criterion 25.4*** – While trusts and similar legal arrangements may not be set up under Croatian law, natural or legal persons resident or established in Croatia may still act as trustees in respect of foreign trusts or similar legal arrangements. Such services would typically be carried out by legal or accountancy professions. Other natural persons may provide trustee services and would be considered as REs (AMLTFL, Art. 9(2)(17)), however, the authorities have indicated that at the time of the evaluation, there were no such trust service providers.

There are no legal provisions under the AMLTFL preventing trust service providers, legal or accountancy professions from providing BO information or other information on trusts and legal arrangements they service to competent authorities or other REs. Deficiencies exist regarding protection of directors see R.21.1

As explained under c. 25.3 trustees are bound to provide to REs BO information of trusts or similar legal arrangements for which they would be acting. Moreover, as set out under c.10.19, the provision of CDD information is necessary for the establishment and continuation of a business relationship with or the carrying out of an occasional transaction for a trustee acting on behalf of a foreign trust or similar legal arrangement.

Pursuant to AMLTFL (Art. 113(1-2)), the AMLO may request trustees or persons acting in similar positions in respect of other legal arrangements (as REs) to provide, upon request, all additional data, information and documentation, which includes, inter alia, data and information collected or held by the trustee on the customer, including banking and financial documentation. These provisions are considered to cover both information on BO, as well as information on assets held in trust.

As set out under c.11.4, it is not clear how CDD and transaction records would be accessible to supervisory authorities (except the CNB) for AML/CFT purposes and law enforcement authorities. In the absence of a clear legal power for these authorities to obtain information on trusts or legal arrangements serviced by REs, it is doubtful whether trustees may be exempt from professional secrecy and compelled to provide such information.

Moreover, accountancy professionals are not regarded as REs when providing trust services (see R. 22). Hence it is likewise doubtful whether they would be bound to provide information on clients (trusts or similar legal arrangements) to competent authorities.

***Criterion 25.5*** – BO information, including information on trustee(s) of foreign trusts that are serviced by trustees resident/established in Croatia, and of foreign trusts that are serviced by trustees resident/established outside the EU but acquire real estate or establish business relationships with Croatian REs, is required to be registered in the BO Register. This also applies to foreign legal arrangements similar to trusts and persons holding functions akin to trustees in these arrangements (see c.25.1), subject to derogations where proof of EU registration can be provided.

In accordance with Art. 34 paragraph 1 of the AMLTFL (and complemented by more detailed provisions under the Rulebook) the register of BOs is accessible to the AMLO, supervisors and other services within the MoF (i.e., Financial Inspectorate, TA and CA), the CNB, CFSSA, the SAO,

the SIA, the MoI (which includes the Police) and other state authorities and various government ministries.

It is questionable how the availability of BO information of foreign trusts on the register of beneficial information is being ensured (see c. 25.1).

CDD and other customer records (which would include BO information of foreign trusts/legal arrangements and assets held under such trusts/legal arrangements) retained by Croatian REs are accessible to the AMLO, although within 15 days from making a request which is not considered timely although, in practice, this is normally shorter see R24.6. It is not clear how these records are accessible to most other supervisory authorities for AML/CFT supervision purposes and law enforcement authorities (see c. 24.6 and c. 11.4). Moreover, accountancy professionals are not regarded as REs when providing trust services (see R. 22). Hence it is doubtful whether they would be bound to provide CDD and other customer records on clients (trusts or similar legal arrangements) to competent authorities.

***Criterion 25.6*** – No trusts or similar legal arrangements may be set up under Croatian Law. However, the Croatian BO Register could hold BO information of certain foreign trusts (see c. 25.1).

Competent authorities having access to such Register are empowered to exchange information obtained through the Register with their foreign counterparts.

Analysis and deficiencies identified in R. 37–40 are relevant in relation to the exchange of information on foreign trusts/legal arrangements that may be obtained through Croatia REs.

***Criterion 25.7 –*** Art. 153 paragraphs 10 and 11 of the AMLTFL prescribe sanctions for trustees (and persons holding a similar role in respect of other legal arrangements) which do not adhere to their obligations to hold accurate and updated BO information and to provide such information to the register of BOs in a timely manner (obligations explained under c.25.1). Under these paragraphs, fines ranging from HRK 5 000 (EUR 670) to HRK 75 000 (EUR 10 000) may be imposed on such trustees. Paragraph 12 provides that for the most severe types of contraventions (and where proceeds are gained or damage caused), the maximum fine on the trustee may increase up to HRK 100 000 (EUR 13 000). The authorities explained that contraventions would typically be considered more severe where the non–provision of BO information is intentional, aimed at concealment of the real beneficiaries. However, this is not set out in any policy document or procedures. The range of these sanctions are not considered by the assessment team to be dissuasive.

Sanctions are also available under the AMLTFL for REs (including Croatian trustees or REs administering or providing services to foreign trusts/legal arrangements), members of the management board and responsible persons of such REs for failure to carry out their AML/CFT obligations under the AMLTFL including the identification and verification of BOs and the retention of CDD information (including BO information). Given that accountancy professionals are not considered REs when providing services to trusts or similar legal arrangements, these sanctions would not apply in their regard.

***Criterion 25.8*** – Sanctions are available under Art. 150(59) of the AMLTFL for REs' (including resident trustees administering foreign trusts or similar legal arrangements) failure to provide information (as explained under c. 25.4) to the AMLO within the stipulated timeframes.

Fines under Art. 150 may range from HRK 35 000 (EUR 4 700) to HRK 1mln. (EUR 134 000) and may go up to HRK 7 500 000 (EUR 1mln.) or HRK 38 000 000 (EUR 5mln.) (in case of credit or

financial institutions) or double the amount of proceeds made from a breach or 10% of the annual turnover in the case of the most severe misdemeanours. Fines vary depending on the type and severity of the breach and the legal status of the perpetrator (see R.35)

Moreover, the AMLTFL (Art. 153(17–18)) prescribe sanctions for trustees of a foreign trust or similar legal arrangement if, upon the request of the TA, such a trustee fails to submit to the TA written documentation on the basis of which the ownership and control structure can be determined, and information collected on the BO. Sanctions under these paragraphs range between HRK 5 000 (EUR 670) and HRK 75 000 (EUR 10 000), or HRK 100 000 (EUR 13 000) in case of the most severe misdemeanours. Under 11.4, it is set out how supervisors supervising REs can obtain CDD and transaction records held by REs. Sanctions for failing to provide supervisors with information requested are set out in AMLTFL and various Supervisory and sector–specific laws, and penalties range from fines of HRK 5 000 to HRK 1mln. (EUR 670 to 134 000), fines of a % of overall income and withdrawal of authorisation. Where data is legally protected by banking secrecy or Credit Institutions Law data can be divulged to States attorney's office, to the Office for the Prevention of Corruption and Organised Crime and to the MoI (which includes the Police) in criminal or preliminary proceedings, when requested or ordered in writing by the SAO, by the competent Court or the competent authority of EU–Member State.

### *Weighting and Conclusion*

Trusts under Croatian law are not permitted, and examples of misuse in the NRA relates to legal persons not legal arrangements and on–site RE's rarely reported encountering foreign trusts. The requirements imposed by Croatia regarding the registration of foreign trusts buying property or establishing a business relationship with Croatian REs, that there are no such registrations by November 2020, which is supported by the lack of issuance of PIN. Registration is not a requirement of R25. As at November 2020, there are no recorded trust service providers. A deficiency is that accountants are not considered REs when providing services to trusts or legal arrangements. **R.25 is rated as LC.**

## *Recommendation 26 – Regulation and supervision of financial institutions*

In the 4th round MER of 2013, Croatia was rated PC on R.23. The main deficiencies were related to deficiencies in fit and proper checks and other measures related to preventing criminals from holding (being beneficial owner of) shares or managerial positions in financial institutions, holding a controlling interest or management function in financial institutions; no licensing or registration for money and value transfer (and other financial) services offered by the Croatian Post; and, lack of legislatively defined licensing requirements and procedures for business entities engaged in factoring activities.

***Criterion 26.1*** – The CNB is the designated regulatory authority for the licensing of banks, saving banks, housing saving banks, credit unions, payment institutions, electronic money institutions, foreign exchange operations and the operation of authorised exchange offices and MVTS (CNB Law, Art.4(1)). The CNB also has supervisory responsibility for banks, saving banks, housing saving banks, credit unions, payment institutions and electronic money institutions. The Financial Inspectorate is responsible for the supervision of authorised exchange offices and the MVTS. The CFSSA is the designated licensing/regulatory authority for REs dealing with insurance, investment, asset management, leasing and factoring, and VASPs (CFFSA Law, Art.15(1–7) and AMLTFL, Art.9(2(6–13) and Art.9(17)(k–l)). The HP–Croatian Post is regulated by the Croatian Regulatory Authority for Network Industries (Postal Services Law, Art.5(3) and Art.7), The

Croatian Bank for Reconstruction and Development is set up by the law and regulated by the Government (CBRD Law). In addition to this, the CNB, the CFSSA and the MoF (under which the Financial Inspectorate falls) are empowered to issue Rulebooks and guidance for the FIs (See Rec. 34). The three supervisory authorities are also designated authorities to ensure compliance of FIs, including foreign FIs' branches, representations and distributors, with the AMLTFL and regulations adopted pursuant to it (AMLTFL, Art.81(1), 82(1–2)(5)).

The CNB, the CFSSA and the MoF are designated bodies for supervision of implementation of the EU and UN TFS (IRM Law, Art.13), Government Decision N 50301–21/21–14–2).

***Criterion 26.2*** – Core Principles FIs: The following core principle institutions are required to be authorised by the CNB and the CFSSA: banks, saving banks, and housing saving banks (Credit Institutions Act, Art. 60–63), credit unions (Credit Unions Act, Art. 2 and 31), life insurance companies (Insurance Act, Art.24), investment fund management companies and investment funds (OEIFPO Law, Art.23, and AIF Law, Art.28), investment companies (Capital Markets Act, Art.38).

Other FIs are required to be authorised by the CNB and the CFSSA: E–Money Institutions (Electronic Money Act, Art.18), Payment Institutions (PSL, Art.86), MVTS (PSL Art.140(1) and (6)), exchange offices (Foreign Exchange Law (FEL) Art.46) Leasing companies (Leasing Act, Art.3) and Factoring companies (Factoring Act, Art.20). Croatian Post is a state–owned postal service – HP – Hrvatska pošta d.d., in addition to being an agent of Western Union, also provides money or value transfer services via postal orders. Its activities are regulated by the Law on Ratification of the Agreement for Postal Payment Services and supervised by the Financial Inspectorate.

The AMLFTL prohibits FIs from establishing or maintaining correspondent relationships with a shell bank. Whilst there is no explicit prohibition whereby a shell bank is not allowed to establish or continue operations within Croatia, the nature and requirements of Croatia's licensing and regulatory process would prevent such to be established in the jurisdiction, e.g., Art.67 of the Credit Institutions Law sets out the conditions for authorisation which includes the need for a credit institution to have a physical presence in Croatia.

***Criterion 26.3 –*** All 3 supervisory authorities of FI's, the CNB, the CFSSA and the Financial Inspectorate, are required to prevent criminals and associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a financial institution. This is done via requirements set out in the sectorial laws that prevents supervisory authorities from approving an individual with a criminal history.

Art.35 of the Credit Institutions Law requires credit institutions to have a management board and a supervisory board, and these individuals are required to be of good repute, and this includes the need to take into account whether the person has been convicted by a judgement with final force and effect or an investigation has been initiated, as per Art.38. The CNB is required to approve individuals holding a function within a management board (Art.39) and Supervisory board (Art.46). In respect to the management board, Art.38(4) notes that a person who is convicted of a criminal offence or is an associate of a person who has been convicted of a criminal offence; is not considered of good repute. In respect to qualifying holdings, Art.4(1) of the Decision on the approval to acquire a qualifying holding in a credit institution (banks, saving banks, housing saving banks) notes that the CNB is required to assess the good repute of associates of the acquirer, and acquirers would be considered to lack integrity if convicted of a criminal offence or if it's associates lack integrity (Art.4(7)).

Art.16 of the Decision on the assessment of the suitability of the chairperson of the management board, members of the management board, members of the supervisory board and key function holders in a credit institution (banks, saving banks, housing saving banks); imposes a requirement on the chairperson, management board and supervisory board individuals to submit questionnaires annually, updating the personal information that includes information on any criminal offences, investigations, etc.

With respect to payment services and electronic money, the PSL and the Electronic Money Law, sets out the provisions for the granting of authorisation, including the assessment of the suitability of a holder of a qualifying holding. The assessment requires the CNB to take into account the repute of the holder of a qualifying holding, and this includes the need to take into account whether the person has been convicted by a judgement with final force and effect or an investigation has been initiated. This extends to criminal associates in Art.84(3)(3) and Art.16(3)(3), respectively. The approval is required for any changes to a qualifying holding, defined in Art.119 of the PSL.

Authorised Exchange Offices: Whilst supervised by the Financial Inspectorate, the CNB is responsible for the fitness and propriety of key individuals within the regulated exchange offices. The supervisory act, FEL, governs the provisions to approve qualifying holdings, those exercising a significant influence, and management bodies and the requirement to take into account criminal convictions and investigations, including the association to criminals.

In respect to the activities supervised by the CFSSA and Financial Inspectorate, the various Acts applicable cover the requirement for the relevant supervisory body to approve qualifying holdings, those exercising a significant influence, and management bodies. As part of the approval and criteria to be approved, this includes the requirement for the supervisory body to take into account criminal convictions and investigations, including the association to criminals. The laws are prescriptive and prohibit the approval of individuals to a key function position if the individual has a criminal history and is not an associate of a person convicted of a criminal offence.

***Criterion 26.4 –*** Croatia completed a self–assessment against Basel Committee Principles in May 2021. The assessment was carried out independently by the CNB's internal audit team and has clearly documented the scope and methodology. The assessment evidences the CNB's compliance with the Basel Core Principles, scoring compliant or largely compliance for all principles. For those principles scored as largely compliant, an action plan has been agreed to address the deficiencies.

Furthermore, the authorities have provided the assessment of the IOSCO Principles 2 and 3 and an assessment against IAIS Principles 4–5 and 7–8. These assessments partially cover the principles indicated in the FATF Standards. For those principles assessed, Croatia appears to be largely in line with the core principles.

For AML/CFT purposes Croatia's supervisory framework does not differentiate between core principles and non–core principles FIs, therefore, all supervisory authorities are obliged to apply an ML/TF risk–based approach to all REs under its supervision. The AMLFTL (Art.84) sets out the primary requirements for the supervision and risk assessment of all FIs that fall within the scope of the Law, including core principle financial institutions.

When dealing with the FI group supervision on AML/CFT matters, powers of the CNB and CFSSA are limited to instances where the financial group is a part of a foreign FI (AMLTFL, Art.85). Other respective provisions that deal with the group structures within the scope of the AMLTFL seem

to follow the same logic – the group, not including the scenario of a domestic structure only (AMLTFL, Art.62 and 83a).

***Criterion 26.5*** – When planning and implementing the supervision of FI's, supervisory authorities should apply a risk–based approach based on the frequency and intensity of on–site and off–site supervision on the risk profile of the FI, and the ML/FT risks present in Croatia, as provided in the NRA (AMLTFL Art.84(1–2)). When planning and performing the supervision, the CNB, the Financial Inspectorate and the CFSSA should adhere to the EBA Guidelines on AML/CFT Supervision (AMLTFL, Art.84(5)).

The CNB has demonstrated intensive on–site and off–site work on Banks. Whilst other credit institutions, i.e., credit unions and house savings banks, together with E–money and Payment Institutions, have primarily been the focus on off–site supervision since 2016. Nonetheless, the off–site supervision is on par with on–site inspections.

Similarly, the Financial Inspectorate has focused its resources on the supervision, particularly on–site inspections, of MVTS and Authorised Exchange Offices.

With respect to the CFSSA, the on–site frequency and intensive is deficient, as can be evidenced in IO.3. Supervision is partially addressed through off–site work.

This covers the factors to be considered by supervisory authorities as part of their own risk assessment, which in turn determine the supervisory plan of an FI. The factors do include internal controls, e.g., internal governance and compliance culture, and characteristics of the RE, e.g., type of customers and jurisdictions of activities. The characteristics of the FI or a group to be considered are provided in the EBA Guidelines on AML/CFT Supervision.

***Criterion 26.6*** – The AMLTFL (Art.84) sets out the requirements for supervisory authorities to ensure that they base the frequency and intensity of direct and indirect supervision on the risk profile of the RE and on ML/TF risks identified in Croatia, based on the NRA. Furthermore, supervisory authorities are obliged to revise the assessment periodically and when important changes occur in the business processes and business practice or the development in the management and operations.

The requirements in Art.84 refer to the RE and not to group, as required by the FATF Standards.

### *Weighting and Conclusion*

Group supervision is limited to instances where the financial group is a part of a foreign FI only. Furthermore, there are no supervisory requirements to consider the group as part of the supervisory authorities' risk assessment of FIs. Lastly, the CFSSA's supervision is considered deficient. **R.26 is rated LC.**

## *Recommendation 27 – Powers of supervisors*

In the 4th round MER of 2013, Croatia was rated "C" on R.29.

***Criterion 27.1*** – The CNB, Financial Inspectorate, and CFSSA are vested with powers to supervise and ensure compliance by the FIs with the AML/CFT requirements, as set out in the AMLTFL and regulations adopted on its basis, and also, with the IRM Law (AMLTFL, Art.81, 82, 83, IRM Law, Art.13, and Government Decision N50301–21/21–14–2).

***Criterion 27.2*** – Provisions permitting the CNB, Financial Inspectorate and CFSSA, to carry out on–site and off–site supervision, is stipulated in the AMLTFL (Art.84(2(3)).

Furthermore, there is sectorial legislation that also provides the designated authorities with the powers to carry out on–site and off–site supervision. These are: in respect to the CNB – credit institutions (Credit Institution Law, Art.175(1) and 177(1)), credit unions (Credit Unions Law, Art.50 and 51), payment institutions (PSL, Art.111(1)), electronic money institutions (Electronic Money Law, Art.48(1)). In respect to the CFSSA – investment funds and investment fund management companies (AIF Law, Art.232(1) and 234; and the OEIFPO Law, Art.346(1) and 348); pension companies (Voluntary Pension Funds Act, Art. 275(1) and 276, Pension Insurance Companies Act, Art. 136 and 139); firms providing investment services (Capital market Act, Art. 192, 685 (1–2)); life insurance companies, life insurance intermediation companies, insurance agents entering into life investment – related insurance (Insurance Act, Art. 203(1), 204(3) and 219(1–3)), factoring companies (Factoring Act, Art. 72(1) and 75), and leasing companies (Leasing Act, Art. 78(1) and 81). In respect to the Financial Inspectorate – the Financial Inspectorate Law, Art.3 and 12

***Criterion 27.3*** – CNB: Art.67(6) of the AMLTFL does impose the obligation on FIs, subject to the supervision of the CNB, to provide reports and information as requested. And states this requirement as a misdemeanour in Art.150 of the Act. Furthermore, Art.153 of the Credit Institution Law stipulates that credit institutions are required to submit reports or other information at the request of the CNB.

Financial Inspectorate: Authority for compelling information by the Financial Inspectorate from FIs is stipulated in the Financial Inspectorate Law, Art.10.

CFSSA: Authority for compelling information by the CFSSA from FIs is stipulated in the sectorial legislation for: pension companies (Voluntary Pension Funds Act, Art. 275(4) and 278, Pension Insurance Companies Act, Art. 138 and 143); investment services providers (Capital market Act, Art. 684, AIF Law, Art 232(5) and 236, and OEIFPO Law, Art. 346(4) and 350; life insurance companies, life insurance intermediation companies, insurance agents entering into life investment – related insurance (Insurance Act, Art. 221), factoring companies (Factoring Act, Art. 72(4) and 77), leasing companies (Leasing Act, Art. 78(4) and 83).

***Criterion 27.4*** – The AMLTFL (Chapter VIII) sets out the overarching provisions to impose monetary fines on REs. The Council for Misdemeanour Proceedings, as the authority responsible for dealing with misdemeanour proceedings, is the only authority able to impose monetary fines and the banning of individuals from holding key functions under the AMLTFL. Supervisory authorities, including the AML/CFT Supervisory team within the Financial Inspectorate, may submit a proposal/indictment for the commencement of misdemeanour proceedings (AMLTFL, Art.83), however, this will be at the Council for Misdemeanour Proceedings' discretion.

All supervisory authorities have the legal powers to impose sanctions directly on REs under Art.233 and 228 of the Misdemeanour Law.

Art.83 of the AMLTFL provides all supervisory authorities with powers to; 1) issue written warnings to address deficiencies in compliance, 2) temporarily prohibit activity, 3) temporarily ban a person from holding a key function, 4) withdrawal of authorisation or approval of a person.

The deficiencies identified within R.35 limit compliance with this criterion.

### *Weighting and Conclusion*

Deficiencies are only in respect to the impact of R.35. **R.27 is rated LC.**

### *Recommendation 28 – Regulation and supervision of DNFBPs*

In the 4th round MER of 2013, Croatia was rated LC on R.24. The only deficiency was the lack of specific provisions for preventing criminal associates from holding a significant interest in casinos.

***Criterion 28.1*** – Organisers of games of chance are designated as REs. These include lottery games, casino games, betting games, slot–machine gaming and games of chance on the Internet and via other telecommunications means, i.e., electronic communications (AMLTFL Act, Art. 9 (16)). They are required to implement respective AML/CFT measures, as set out in the AMLTFL and by–laws (AMLTFL, Art. 11(1))[230].

(a) Organisers of games of chance are required to be licensed by the decision of the Government of the Republic of Croatia upon the proposal of the MoF (Games of Chance Law, Art.23).

(b) Proof of no criminal proceedings against the director, founders of the company, BOs, and supervisory board members should be presented at the stage of incorporation (Games of Chance Act, Art.24(1(8)). However, there is no explicit provision requiring the supervisory authority to prohibit the appointment to a key function, or the approval of a licence, if an individual has a criminal background or is part of a criminal investigation. Furthermore, there is no requirement preventing criminal associates from holding any of the above–mentioned functions nor to ensure that information on criminal records or association with criminals would be ensured at any time after acquiring the licence.

(c) The designated body for conducting the AML/CFT supervision of all types of organisers of games of chance is the TA (Games of Chance Law, Art.70(1),(4)), AMLTFL, Art. 82(6)). Statutory powers to carry out the supervision of the implementation of the EU but not UN TFS is regulated pursuant to the IRM Law (Art.13), and the Government Decision (N50301–21/21–14–2).

***Criterion 28.2*** –The Financial Inspectorate is the designated authority to ensure compliance of DNFBPs, including foreign DNFBPs' branches, representations and distributors, with the AMLTFL and regulations adopted pursuant to it. (AMLTFL, Art. 81(1), 82(2)). This, however, does not amount to ensuring implementation of the AML/CFT requirements in a broader sense. Statutory powers to carry out the supervision of the implementation of the EU but not UN TFS is regulated pursuant to the IRM Law (Art.13) and the Government Decision (N50301–21/21–14–2).

***Criterion 28.3*** – All DNFBPs[231] are subject to monitoring by a designated competent authority. The Financial Inspectorate is the designated supervisory authority for the supervision of AML/CFT compliance of the DNFBPs[232] other than casinos (AMLTFL, Art.81).

Some limited deficiencies in the scope of the DNFBPs (See C28.2), however, impact the supervisory framework.

***Criterion 28.4*** – Financial Inspectorate carries out supervision of the DNFBPs, other than casinos (AMLTFL, Art.82(2)). Licensing of different types of DNFBPs is distributed among various bodies, as follows: Croatian Bar Association for lawyers, the Ministry of Justice, with the assistance of the

---

[230] This report assesses solely the activities of casinos (land– and internet based) as it is foreseen by the FATF Recommendations. Other gambling activities like betting or lotteries are excluded.

[231] Auditors, tax advisors and dealers in works of art are also covered by the AMLTF–Law, and supervised by the Financial Inspectorate, although they do not fall under the FATF definition of DNFBPs.

[232] Auditors, tax advisors and dealers in works of art are also covered by the AMLTF–Law, and supervised by the Financial Inspectorate, although they do not fall under the FATF definition of DNFBPs

Croatian Notaries Chamber for notaries public (Notary Public Law, Art.14), Croatian Chamber of Commerce for real estate agents.

(a) Authority for conducting inspections by the Financial Inspectorate in DNFBPs on the matters related to AML/CFT, which includes carrying out on–site and off–site supervision, is stipulated in the AMLTFL (Art. 84(2(3)) and in the Financial Inspectorate Law (Art.3 and 12).

(b) The licensing/registration requirements are provided for lawyers, notaries public, and real estate agents. No requirements are set for licensing or registration of the accountants, DPMS and TCSPs. All these sectorial requirements cover provisions for the fitness and property of individuals limited to the checks of a criminal background of the lawyers, and notaries public, respectively. The legislation regulating the conditions for including the real estate agent into the register maintained by the Croatian Chamber of Commerce does not contain requirements for the real estate agent criminal background check. There are no provisions ensuring that information on criminal records or association with criminals should be monitored at any time after acquiring the license/enrolment. Nevertheless, application of a criminal sanction for lawyers, notaries public, and real estate agents is a basis for a termination of their license/registration. (Legal Professions Law, Art.46, 48 and 49; Notaries Public Law, Art. 13 and 14; Real estate brokerage law, Art. 8). There are also no provisions that would concern checks on persons holding (or being the beneficial owner of) a significant or controlling interest or holding a management function. There are no provisions in place with respect to preventing criminal associates from being professionally accredited.

(c) the Financial Inspectorate, when determines violations of the provisions of the AMLTFL and by–laws, is authorised to apply the following types of sanctions: written warning; fine; temporary prohibition of certain business activities by the DNFBPs or their management; prohibition of carrying out certain duties, activities or tasks by the DNFBPs; revocation of license; other measures stipulated by the AMLTFL (Art. 83). Fines are provided for various violations under the AMLTFL (Chapter VIII). There are no similar provisions for application of other types of sanctions for a specific violation of AMLTFL and respective by–laws. The deficiencies identified within R.35 limit compliance with this criterion.

***Criterion 28.5*** – When conducting supervision of DNFBPs, the TA and Financial Inspectorate should apply a risk–based approach (AMLTFL, Art.84(1)), including: determine the frequency and intensity of direct and indirect supervision on the basis of the ML/TF risk identified in the NRA. Supervisory authorities shall take into consideration the discretionary right of the RE when carrying out its risk assessment, and they may, if necessary, appropriately revise the risk assessment of REs. (AMLTFL, Art.84(4)).

The Financial Inspectorate applies a combination of on–site and off–site work, in addition to the collation of data periodically. It focuses its limited resources on high– risk sectors and REs. With respect to the TA, the on–site frequency and intensive is deficient, as can be evidenced in IO.3.

### *Weighting and Conclusion*

There are no provisions prohibiting criminals or their associates from holding a key function within an RE, nor for ensuring that information on criminal records or association with criminals would be ensured at any time after approval of a licence. Supervisory powers do not extend to supervision of the implementation of UN TFS measures. There are no licensing requirements and hence no designated licensing authorities for accountants, DIPM and TCSPs. **R.28 is rated as LC.**

### *Recommendation 29 – Financial intelligence units*

In the 4th round MER of 2013, Croatia was rated C on R.26.

***Criterion 29.1*** – The AMLO is the central national administrative unit responsible for receiving and analysing the reports on suspicious transactions and other information related to money laundering, associated predicate offences and terrorist financing (AMLTFL, Art.101(1)).

The AMLO is responsible for disseminating the results of its operational analyses as financial–intelligence data and all other relevant information to competent authorities for their further actions and processing when there are reasons for the suspicion of ML/TF and associated predicate offences (AMLTFL, Art.101(1) and Art.138(1)).

***Criterion 29.2*** – The AMLO is the central agency for receiving disclosures filed by the REs, including:

(*a*) STRs filed by REs, including the those performing independent professional activity (AMLTFL, Art.56(2), 57(1–3)).

(b) other disclosures in line with the AMLTFL and the relevant legislation – (i) CTRs equal to or exceeding HRK200 000 (EUR27 000) (AMLTFL, Art.61(1)); (ii) reports on cash crossing the EU external border amounting to or exceeding EUR10 000 (AMLTFL; (iii) Art.121(1)), reports on undeclared cash when the amount equals to or exceeds EUR10 000 (AMLTFL, Art.121(2)); (iv) reports on cash regardless of the amount in case of any sort of suspicion of ML or TF (AMLTFL, Art.121(3)); (v) customer's request for advice in relation to ML/TF from REs performing an independent professional activity (AMLTFL, Art.57(3)).

***Criterion 29.3*** – (a) The AMLO is empowered to request any additional data, information and documents from the REs necessary for performing its operational and strategic analysis (AMLTFL, Art.113(1–4)).

(b) The AMLO is empowered to request information from state authorities, courts, local and regional self–government units and legal persons with public powers (AMLTFL, Art. Art. 101(1) and 115(1–2)). State authorities, courts and legal persons with public powers are obliged to provide the AMLO with timely direct or indirect access to financial and administrative data, information and documents, including information on detection and prosecution of criminal offences, and the criminal records (AMLTFL, Art.116(1)).

***Criterion 29.4*** – (a) The AMLO performs operational analysis of suspicious transactions and other accessible and obtainable information for detection of suspicious cases, persons, transactions and assets involved in ML/TF and associated predicate criminal offences (AMLTFL, Art.111(1)).

(b) The AMLO carries out strategic analysis of the received and collected data from REs and the data delivered by competent authorities and foreign financial intelligence units to identify ML/TF related typologies, patterns and trends. (AMLTFL, Art.111(2))

***Criterion 29.5*** – The AMLO is able to disseminate spontaneously, and upon request, information and the results of its analysis, including the operational analysis of suspicious transactions, to competent authorities. Information is provided in a written form or via secure communication channels (AMLTFL, Art.102(1(1)), 123, and 138(1)). The authorities advise that when disseminating in a hard copy, it is done in a sealed envelope by a dedicated employee thus ensuring, that unauthorised access or tampering is prevented.

***Criterion 29.6*** – (a) The AMLO is obliged to protect data, information and documents by adopting internal instructions on security and confidentiality of information, including procedures for handling, storage, dissemination and protection of information, as well as on the access to information and the AMLO's premises (AMLTFL, Art.142(1(1)). The AMLO has issued more than 20 internal instructions dealing with various aspects of protection of information confidentiality and secrecy.

(*b*) All the employees of the AMLO are civil servants and are led by the regulations on civil servants that also cover matters related to requirements on confidentiality of information (AMLTFL, Art.103). Employees holding key positions, such as the head of the AMLO, assistant, heads of organisational units, high–ranking analysts–specialists, high–ranking analysts, and analysts, are subject to vetting (AMLTFL Art.104(2)). All employees are obliged to have an appropriate level of certificate for access to classified data in line with the occupied position and to be appropriately familiar with responsibilities in dealing with classified, non–classified and other data, information and documents, including disseminating classified data to competent states authorities and foreign FIUs (AMLTFL Art.142(2)). All employees are also required to keep confidential all information available within the scope of their duties, including after leaving the AMLO (AMLTFL, Art.144).

(*c*) The AMLO is required to restrict access for unauthorised persons to the premises, data, information and documents, including access to the IT system of the AMLO (AMLTFL, Art.142(1(2)). The other organisational units of the MoF are restricted to access to business premises, data and information and the IT system of the AMLO (AMLTFL, Art.102(1(2)).

***Criterion 29.7*** – (a) The AMLO is authorised to completely fulfil its functions, including the independent decision–making on analysing, making requests, forwarding and disseminating the results of its operational analyses and specific information, data and documents to competent authorities and foreign financial intelligence units (AMLTFL, Art.102 (1(1)).

(b) The AMLO is authorised to conclude agreements on the co–operation or establish independent co–operation in exchanging information with other domestic competent authorities and foreign financial intelligence units (AMLTFL, Art.102(1(5)).

(*c*) The AMLO operates within the MoF as an organisational unit that independently performs basic and other tasks prescribed by the AMLTFL. It has separate key functions from those performed by other organisational units of the MoF (AMLTFL, Art.102(1(2)).

(*d*) The AMLO is authorised on an individual and routine basis to obtain and deploy the resources needed for the performance of its tasks, without any undue political impact or impact of the private sector or disturbance thereof, in order to ensure the full operational independence of the AMLO (AMLTFL, Art.102(1(4)). The AMLO shall be provided with appropriate funds, staff capacities, IT and technical equipment for carrying out its basic and other tasks prescribed by the AMLTFL (Art.102(1(3)).

***Criterion 29.8*** – The AMLO became a member of the Egmont Group in 1998.

*Weighting and Conclusion*

Croatia has successfully implemented all the requirements under this recommendation. **R.29 is rated as C.**

### *Recommendation 30 – Responsibilities of law enforcement and investigative authorities*

In the 4th round MER of 2013, R.27 was not reassessed due to the requirement of the MONEYVAL's 4th round Rules of Procedure. The rating LC in the 3rd round MER (2008) was maintained. The only deficiency identified by the assessment team was related to effectiveness, i.e., lack of convictions or final decisions in any ML case since 2003. Since the adoption of the 3rd and 4th round MERs of Croatia, the FATF Methodology has significantly changed, and most of the requirements under R.27 that used to be additional elements are now obligatory.

***Criterion 30.1*** – In Croatia, designated law enforcement authorities that have responsibility to investigate ML, associated predicate offences and TF offences are the General Police Directorate of the MoI and the SAO.

*The General Police Directorate*

Police conduct an initial investigation into an offence, using a range of intelligence and evidence gathering powers to build a case suitable for referral to the competent State Attorney, and/or undertakes respective measures upon the request of the State Attorney.

Within the General Police Directorate, the Criminal Police Directorate (at the national level) and Police Administrations (at regional level – Police Districts, and at the local level – Police Stations) are the main structural units responsible for investigating ML, TF and the predicate offences (including the list of designated offences as provided in the FATF Standards) (Police Law, Art. 8, and PDPL, Art.11).

In the Criminal Police Directorate, the PNUSKOK, the General Crime and International Police Co–operation Sector and the Criminal Intelligence Sector are in charge of directly investigating complex criminal cases at the national level. This includes investigation of ML, terrorism, including a TF, corruption, organised crime, and other predicate offences (Regulation on Internal Organisation of the Ministry of Internal Affairs).

Within the PNUSKOK, there are several specialised departments established that are dealing with specific types of criminal activity, such as the Terrorism Service, Economic Crime and Corruption Service, Organised Crime Service, Drug Crime Service, and Services for the Suppression of Corruption and Organised Crime (Zagreb, Rijeka, Split and Osijek). Within the General Crime and International Police Co–operation Sector is respectively the General Crime Service, and within the Criminal intelligence sector is the Cyber Security Service (Regulation on Internal Organisation of the Ministry of Internal Affairs, Art.54, 64 and 75).

*State Attorney's Office*

In Croatia SAO supervises the Police actions and leads criminal investigations and all criminal offences (CPC, Art.38(2)). Within the SAOs' competences are split among the County SAO, Municipal SAO, and the USKOK.

The USKOK is a specialised department within the SAO with the competences to investigate ML (if offence was committed in connection with offences determined in Art. 21(2(1–3)); Criminal Association; Corruption and bribery (some of which, if the offence was committed by the official); Tax or Customs Duty Evasion (if was conducted in conjunction with offences provided under Art. 21(2(1–3)), and other offences (USKOK Law, Art.21).

Investigation of other criminal offences is distributed between the County and Municipal SAOs, where the TF and other terrorism–related offences are dealt with by the County SAOs, and the

ML, other than that falling under the competence of the USKOK is dealt with by the Municipal SAOs (CPC Art. 19a (1) and Law on State Attorney Art. 29 (1)).

***Criterion 30.2*** – In Croatia, the parallel financial investigation is conducted where there are grounds to suspect that the criminal activity generated proceeds (CPC, Art.206i(1)) regardless of where the predicate offence occurred. If so, the State Attorney shall immediately undertake investigation or order to police or Tax authorities to launch one, to determine the value and location of the proceeds, and if ML suspicion – also to confiscate the proceeds (CPC, Art.206h(1), and Art.206i(1)).

In addition, if any state authority, including the Police and TA, becomes aware of proceeds generated as a result of criminal conduct or indication of ML, they should without delay inform the State Attorney of those circumstances and provide information in order to follow up with investigation (CPC, Art.206i(4)). In addition, according to the general principle of prosecutorial investigation, if the financial investigation indicates suspicion of TF – related offence, the case is referred to competent for further criminal investigation (CPC Art.38(2)).

In 2013, Criminal Police Directorate provided to all Police Districts guidelines on conducting parallel financial investigations, ML and confiscation of illegally obtained pecuniary advantage.

***Criterion 30.3*** – The State Attorney shall immediately undertake an investigation to identify and trace criminal assets in order to secure confiscation. The State Attorney can undertake these actions autonomously or order the Police to conduct these (CPC, Art.206h(1), Art.206i(1) and Art.557a). The duty of identifying and tracing the proceeds of crime is also a general responsibility of the Police according to the PDPL (Art–s 3(1)5 and 23(1)5). In this regard, the Economic Crime and Corruption Department within the PNUSKOK is the national contact point for the submission of requests and the exchange of data for the purpose of tracing and identification of proceeds of crime (Simplifying exchange of data between LEAs of the Member States of EU Law, Art.9 (2)). The AMLO can also identify, trace and temporary suspend the assets when it detects ML/TF suspicion (AMLTFL, Art.110).

Once proceeds of crime have been identified and located, the State Attorney shall, without delay, propose to the court to order the seizure of such property (CC, Art.206i (5)).

***Criterion 30.4*** – Although tax authorities are not considered part of law enforcement, they do have an independent Sector for Financial Investigations (TA Law, Art.9(2)) with the responsibility for pursuing financial investigations of the predicate offence. In their performance, they can directly request data or, based on the prosecutor's request. In addition, SAO can appoint an authorised official from TA and CA as an investigator to perform evidentiary actions entrusted to him by the competent State Attorney in accordance with the provisions of the CPC and regulations within the respective administration (TA Law Art.14, and CA Law, Art.22).

***Criterion 30.5*** – There is no dedicated anti–corruption enforcement authority in Croatia. The investigation bodies, such as the SAO, USKOK and PNUSKOK referred to in c. 30.1 are also competent to investigate ML/TF offences associated with corruption offences.

*Weighting and Conclusion*

Responsibilities of LEAs and investigative authorities are in line with the FATF requirements**. R.30 is rated C.**

### *Recommendation 31 – Powers of law enforcement and investigative authorities*

In the 4th round MER of 2013, R.28 was not reassessed due to the requirement of the MONEYVAL's 4th round Rules of Procedure. The rating "C" in the 3rd round MER (2008) was maintained.

***Criterion 31.1*** – The Police and the SAO responsible for investigating ML, associated predicate offences and TF are able to obtain access to all necessary documents and information for use in those investigations (Law on Police Duties and Power (PDPL) Art. 13(1); Law on the SAO Art. 79(1–2); CPC, Art. 38(2) and 207(1)).

The range of tools available to ensure this includes the following:

(a) *The production of records held by financial institutions, DNFBPs and other natural or legal persons* – The State Attorney, when investigating ML, FT, and predicate offence, can request all necessary documents and information (CPC, Art. 206.g(2)) held by the state authorities and legal entities (including banks, financial institutions and DNFBPs), except those that represent secrecy protected by law. Non–compliance with the State Attorney's request is subject to penalties (CPC, Art. 206.g(3)). In case of bank secrecy, USKOK can file a request directly to the bank (USKOK Law, Art. 49). However, other competent prosecutors can file a substantiated request to a court to obtain an order. The court order is mandatory for the bank to process under the threat of a fine (CPC, Art. 265(1)). To obtain records that represent other type of secrecy, state prosecutors or the court have to file a motion to the authority to declassify information or in case of a legal person, the investigative judge or the court before which the hearing is conducted is authorised to make a decision (CPC, Art. 264). Only declassified information can be submitted to the prosecutor and used as evidence.

Furthermore, when conducting a criminal investigation, the Police may inspect the business documentation of natural and legal persons and temporary seize it if it is believed that these will be used for the commission of crime or a product of criminal offence or represent the danger for public safety (PDPL, Art. 71(1) and 72). In the other condition, the police would achieve the production of records through the State Attorney request or the Court order (CPC Art. 38 (2(2) and 206.g).

*(b) Search of persons and premises* – A search shall be conducted with a decision of the investigating judge, by the State Attorney, the investigator or the police authorities (CPC, Art.242). In exceptional cases, where a search needs to be conducted immediately because its postponement would jeopardise the achievement of the goals of the search concerning particularly serious crimes, including TF and ML, it can be conducted with an order of the State Attorney (or directly by the police) (CPC, Art.245). Those exceptions are, e.g., cases of presumed armed resistance; offence committed by criminal organisations or criminals are connected with foreign countries if the search shall be performed suddenly; search in public premisses; suspicion that the prior issuance of a warning would endanger the safety of the person conducting the search; and the owner or possessor of the home or movable property is inaccessible (CPC, Art.244).

*(c) Taking witness statements* – The SAO and the Police are authorised to conduct the evidentiary actions, including examination of a witness as a person who is likely to provide information regarding the criminal offence, the perpetrator and other important circumstances (CPC, Art. 38(2(5)) and Art. 283; PDPL, Art.11(a)). Every person who is called as a witness is obliged to respond to the summons and also obliged to testify (CPC, Art.283(3)). In case of non–compliance with the obligation to testify, witness may be punished (CPC Art.291(2)).

*(d) Seizing and obtaining evidence* – The SAO and the Police have the powers to seize and obtain evidences (CPC Art. 38(2(5)), 206g(2) and 206h(1); PDPL, Art 11a, 13(1(10)).

Additionally, temporary seizure of objects as evidence collecting measures is prescribed under the CPC (Art.262). However, temporary seizure is not applicable to files and other documents of state authorities, the publication of which would violate the confidentiality obligation until decided otherwise by the competent authority.

***Criterion 31.2*** – Undercover operations, intercepting communications, accessing computer systems and controlled delivery are special investigative techniques prescribed under Art. 332 of the CPC. These investigative techniques have to be authorised by the investigating judge or, exceptionally where there is a risk of delay and the State Attorney has reasons to believe that he will not be able to obtain the warrant of the investigating judge on time, it can be decided by the State Attorney, subject to the later confirmation of the judge.

The special investigative techniques can only be used in relation to the offences specified in Art. 334 of the CPC, which includes ML and TF. All designated categories of the predicate offences according to the FATF standards are covered by this provision.

***Criterion 31.3*** – (a) Under Art. 265 of the CPC and Art. 49 of the Law on USKOK competent authorities have access to financial information (see criterion 31.1). This Art. 265 establishes that the judge must decide about the request of the State Attorney for obtaining financial information immediately and, in any case, in a maximum term of 12 hours.

The FINA keeps the Centralised Account Register, which is an electronic database of accounts containing data on all types of accounts of business entities and citizens who opened accounts for doing business, including safe deposit boxes. This Register contains the following data: holder of the bank account and a safe deposit box, residence of the holder, personal identification number, IBAN, name of the bank and opening and closing date (Rulebook on Centralised Account Register, Art. 2). According to the provided information, data contained in this Register does not include the identity of the BO of the account in cases where the BO and the account holder are different.

The SAO has direct access, and Police has indirect access to the Centralised Account Register. Police can obtain this data within hours. The Police also uses the commercial database 'Poslovna Hrvatska' (Business Croatia) for identification of bank accounts, where various data may be found for a fee. These include data on business entities, persons managing the business entities, financial reports in the past five years, data on business performance by key financial indicators, detailed reports on business entities and their managers and data on bank accounts of business entities.

Moreover, in 2014, the TA and the General Police Directorate of the MoI concluded an Appendix to the Protocol on co–operation and exchange of information by which the TA provided access to its records to police officers at national level. This database also contains data on bank accounts of taxpayers (both natural and legal persons).

(b) Criminal proceedings conducted by the Police and the State Attorney within the framework of inquiry, obtaining bank secrecy and ordering suspension of financial transaction are protected by secrecy, and legal and natural persons are prohibited from revealing information or data on these proceedings. This would include the owner of assets (CPC, Art.206f, 265(7), 266(4)).

***Criterion 31.4*** – Competent authorities when investigating ML, associated predicate offences or TF, are able to co–operate with the AMLO (AMLTFL, Art.120). The SAO, the Police, the Court and other competent authorities may submit a substantiated request to the AMLO for conducting

analysis and providing the results of its analysis on suspicion related to ML/TF and associated predicate offences (AMLTFL, Art. 123). A Protocol on the co–operation and the establishment of the Inter–Institutional Working Group for the prevention of ML/TF is signed to ensure coordination of actions of institutions including the SAO, Police, and courts.

*Weighting and Conclusion*

In Croatia, the competent investigative authorities have power to access and obtain information applying various compulsory measures, technics and mechanisms. Some deficiencies, however, are identified with respect to the powers of temporary seizure of files and other documents of state authorities, the publication of which would violate the confidentiality obligation, until decided otherwise by the competent authority. **R.31 is rated LC.**

### *Recommendation 32 – Cash Couriers*

In the 4th round MER of 2013, Croatia was rated LC on SR.IX. In the 4th MER, Croatia had no powers to apply sanctions to persons who made a false declaration and had no requirement to retain some relevant information in some cases. Since July 2013, Croatia is a member of the EU, and in this regard, EU supranational legislation applies.

***Criteria 32.1*** – Croatia has implemented a (written) declaration system for incoming and outgoing transportation of cash (i.e., currency and BNIs) of amounts of a value of EUR 10 000 or more. The general framework of the declaration regime is set forth in the EU Regulation 1889/2005 and is further implemented in Croatia through the FEL. This declaration system has been established on a supra–national basis (European Union) and applies only to movements (both inward and outward) of cash from and to the EU. Croatia does not have a declaration/disclosure system in place for movement of cash and BNI within the EU. The Croatian regulations apply only to natural persons and, therefore, do not cover the physical transportation of cash through container cargo or the shipment of cash through mail. The authorities note that this gap is covered by the entering into force of EU Reg 2018/1672 and Amendments of the FEL, however as this came into force in June 2021 it falls well outside the period under evaluation.

***Criteria 32.2*** – Natural persons entering or leaving the EU through Croatia carrying cash equal to or exceeding EUR 10 000 should make a written declaration to the CA (FEL, Art 40). Deficiencies under c.32.1 equally apply.

***Criterion 32.3*** – Not applicable, as Croatia operates a declaration system.

***Criterion 32.4*** – CA supervises the compliance with the obligation to declare currency or BNIs (FEL, Art.59). The CA officers shall check the submitted documents and have the right to request any additional information from the person obliged to fulfil their duties (CA Law (CSL) Art.32), as well as to check items which they carry (CSL Art. 43) and to monitor, stop, inspect and check transportation vehicle (CSL Art. 48).

***Criterion 32.5*** – The FEL (Art. 69) provides the misdemeanour sanctions for a person who fails to declare attempt of or transportation of cash in the amount of EUR 10 000 or more. A person fails to meet the obligation to declare, as set out in the EU Regulation 1889/2005(Art.3) if the information provided is incorrect or incomplete. A fine between HKR 5 000 to HKR 50 000 (EUR 670 to EUR 6 700) shall be imposed, together with confiscation of and the undeclared cash. In justified cases in which there are particularly mitigating circumstances, there can be applied a partial or no confiscation of cash. However, there are no sanctions for the legal entities (see

deficiency under c.32.1). The assessment team concludes that the sanctions legally provided are not fully dissuasive and proportionate.

***Criterion 32.6*** – The CA shall inform the AMLO of every report of the incoming and outgoing cross–border cash or BNIs transportation in the amount of EUR 10 000 or more; unreported cross–border transportation of cash or BNIs; notify about suspicious cross–border transportation or attempt of transportation of cash or BNIs irrespective of the amount (AMLTFL, Art. 121(1–3)).

The referred information is reported by the CA to the AMLO electronically, using the AMLO's application software and filling in a form that includes information regarding cash, cash courier, cash owner, intended cash recipient, reasons for suspicion on ML/TF and the CA's organisation Unit (Rulebook on the means and extent of reporting cash transport across the state border to the anti–money laundering office by CA).

***Criterion 32.7*** – The CA shall co–operate with state bodies, local and regional self–government units and legal persons having public authority to take measures to achieve the efficient and purposeful performance of the customs services. For this purpose, the CA may conclude a co–operation agreement (CSL, Art. 5). In this regard, two documents were arranged in 2007: (i) a Protocol on co–operation and exchange of information between the MoI, MoF – CA, TA, Financial Police, Financial Inspectorate and the AMLO, and (ii) a Protocol on Co–operation and Establishment of the IIWG.

***Criterion 32.8*** – Under the general powers the CA is authorised to detect, prevent, and suppress misdemeanours and criminal offences, detect and collect data on these offences and perpetrators and implement evidentiary actions in criminal proceedings in accordance with the provisions of the CPC (CSL, Art.4(3(6)). Thus, the competent authorities would be able to stop or restrain currencies and BNI in order to ascertain where the evidence of ML/TF may be found within the powers provided by CPC (CSL, Art.48 and 50–52).

***Criterion 32.9*** – The Central Office of the CA collaborates with competent services of other countries, international organisations and expert associations within its competence (CSL, Art. 11(28)). Croatian authorities co–operate with foreign counterparts (EU Member States and the third countries) following the terms established under the EU Regulation 1889/2005 (Art.–s 6 and 7). Croatia also concluded 15 bilateral agreements which govern customs co–operation. CA participates in the international joint customs operations aimed at preventing ML and controlling legal trans–border cash movements (ATHENA, CERBERUS). In addition, CA at local level utilise powers conferred by the EU Regulation 515/97, which allows the exchange of operational information related to false declarations with other EU member States. Information obtained from the declaration regime is retained by the CA for a period of ten years (AMLCFT Law Art. 122 (2)). CA is obliged to submit information on cash transactions to the AMLO (AMLTF Art. 121), which will keep information for 10 years (AMLTF Art. 145). This information contains data on (i) the amount of currency or BNIs declared and (ii) the identification data of the bearer(s).

***Criterion 32.10*** – As a member of the EU, Croatia shall apply safeguards to personal data privacy as stipulated in EU Regulation no 1889/2005 (Art. 8). Personal data collected by the CA is subject to the regulations concerning personal data protection (CSL, Art. 29(2)). A specifically authorised CA officer submits notifications to the AMLO, electronically. Officers of the AMLO dealing with data, information and documentation, are obliged to keep it secret until they are released in accordance with law (AMLCFT Law, Art.143 (2)). There are no constraints in place limiting trade payments between countries for goods, services or the freedom of capital movements.

***Criterion 32.11*** – Persons transporting cash related to ML/TF or predicate offences are subject to criminal sanctions. Criminal sanctions for ML offences are not proportionate and dissuasive. Criminal sanctions for TF are proportionate and dissuasive. Confiscation mechanisms are regulated under the CC and CPC. Strengths and vulnerabilities of the system, as described under R.4, would equally apply here. Limited scope of the obligation to declare cross–border movement of cash and BNI identified at c.32.1 impacts the compliance with the standards.

*Weighting and Conclusion*

Some of the requirements are implemented adequately. However, regulatory measures apply only to movements (both inward and outward) of cash from and to the EU, these do not extend to physical transportation of cash through container cargo or the shipment of cash through mail. Sanctions are not proportionate and dissuasive enough. **R.32 is rated PC.**

### *Recommendation 33 – Statistics*

In the 4th round MER of 2013, Croatia was rated PC on R.32. The main deficiency was the lack of comprehensive statistics on matters relevant to the effectiveness and efficiency of systems for combating ML/TF relating to MLA and other forms of international co–operation, including the co–operation of LEA and supervisory authorities.

***Criterion 33.1*** – The AMLTFL provides for maintaining of comprehensive AML/CFT–related statistics, as follows:

*(a) STRs, received and disseminated* – The AMLO is obliged to maintain detailed statistics on received and disseminated STRs (AMLTFL, Art.147(1) and (7)). The statistics provided to the assessment team contain information on the STRs received and disseminated to specific authority on large transactions submitted via specific reporting entity, on the numbers of FIU cases in judicial proceedings (including data on prosecutions and convictions) and on cross–border transportation of currency and BNIs (covering declarations, disclosures and suspicious incidents) all divided into type of offence.

*(b–c) ML/TF investigations, prosecutions and convictions; property frozen, seized and confiscated* – In Croatia, the AMLO is the designated authority for collecting and maintaining status on ML/TF and predicate offences in a centralised manner. The Police, State Attorney, CA, the competent courts, and the supervisory authorities – the CNB, CFSSA, the Financial Inspectorate and the TA are obliged to submit the respective statistics regularly (on a semi–annual and annual basis) (AMLTFL, Art.148). These statistics, among others, should include information on ML/TF investigations, prosecutions, and convictions; and property frozen, seized and confiscated.

As concerns the comprehensiveness of statistics that are maintained, Croatia have provided limited data on investigations and prosecutions of a number of criminal offences, including the ML. Croatia does not maintain statistics related to confiscation and the cause of its subsidiary nature. The statistics of judicial activity, therefore, does not include all cases related to confiscation.

*(d) MLA and other forms of international co–operation* – In cases in which the criminal proceeding is conducted for the ML/TF and the associated predicate offences the SAO and the competent court are obliged to deliver the data to the AMLO, twice a year on realised international co–operation, including the MLA (AMLTFL, Art.148(1(5–6) and 3(4)). Croatia keeps statistics on MLA for the designated categories of the offences. In respect to other forms of international co–operation, police maintain statistics (PDPL Art. 4(1), however, there is no clear distinction

between incoming and outgoing requests. CA keeps statistics based on the CSL Art.11(1) and CNB based on the internal act "Procedure for carrying out tasks in AMLTFL Supervision Department". Financial Inspectorate also has internal procedures enabling them to maintain statistics, including international co–operation. The TA and CFSSA do not keep statistics relevant only to international co–operation. However, these legal provisions do not cover other types of international co–operation conducted by the Police, CA, TA, and supervisory authorities on the matters relevant to the AML/CFT system of Croatia. No statistics are maintained on international co–operation carried out by the supervisors aside from the Police, the CNB and the CFSSA. Some statistics on International Police, TA and CA co–operation is collected as a result of membership in the relevant organisations: Interpol, Europol, Egmont, EU Regulation 515/97, Napel II, on co–operation performed within the relevant instruments.

*Weighting and Conclusion*

While Croatia has a solid legislative basis for collecting and maintaining statistics, the effective implementation of this, in practice, was not demonstrated through the submitted information. Croatian authorities do not maintain comprehensive statistics on ML/TF investigations, prosecution, and conviction, as well as data on seizure and confiscation. In addition, there is no legislative requirement for maintaining statistics on international co–operation carried out by the Police, CA, TA, and supervisory authorities. In practice, this is maintained only by the CNB. **R.33 is rated PC**.

### *Recommendation 34 – Guidance and feedback*

In the 4th round MER of 2013, Croatia was rated LC on R.25. The only deficiency was a limited amount of information provided to financial institutions on ML/TF trends.

***Criterion 34.1*** – The AMLTFL provides for a set of requirements for the competent authorities and the AMLO on establishing Rulebooks, guidelines and other respective documents and providing feedback to FIs and DNFBPs.

*Guidelines*

The MoF should adopt Rulebooks on the following matters: (a) procedure for ML/TF risk assessment to support the FIs when conducting the risk assessment of business relationship and occasional transactions (AMLTFL, Art.14(11)); (b) on data to be collected by the REs for conducting CDD and reporting STRs (AMLTFL, Art.20(4)); (c) the manner of the implementation of simplified and EDD by the FIs (AMLTFL, Art.42(1)); (d) minimum technical conditions that the REs should fulfil for video electronic (non–face–to–face) identification of a customer and verification of his identity (AMLTFL, Art.52(6)); and (e) the means and scope of reporting STR, cash transactions and providing additional data by the REs (AMLTFL, Art.59(3), 60(7), 61(3), 113(7)).

In line with the legislative requirements, the MoF adopted the respective Rulebooks. Only Rulebook on mandatory inclusion of individual indicators on the list of indicators for recognising suspicious transactions, funds and persons in relation to which/whom there are reasons for the suspicion of money laundering or terrorist financing, as required under Art. 60(7) is not yet adopted.

The CNB should adopt Rulebooks or decisions on information to accompany transfers of funds (AMLTFL, Art.98) and other matters as provided by the AMLTFL (Art.14(11), and Art.42(1)). The

CNB can also adopt sectorial guidelines for the uniform application of the AMLTFL by REs (AMLTFL, Art.88(1)).

The CNB is issuing decisions, making use of the Risk Factors Guidelines of the ESA. In particular, this refers to a decision on the process of assessing ML and TF risk and the manner of applying simplified and EDD measures, which gives detailed instructions to the supervised REs on the RBA expectations in the course of the business relationship or occasional transaction with their clients. Among others, around 12 Guidelines were issued by the CNB to address specifically the AMLTFL on the matters provided above.

The CFSSA should adopt Rulebooks or decisions on the specific matters stipulated by the AMLTFL (Art.14(11), and Art.42(1)). The CFSSA can also adopt sectorial guidelines for the uniform application of the AMLTFL by REs (AMLTFL, Art.88(1)).

Similar to the CNB, the CFSSA is issuing decisions, making use of the Risk Factors Guidelines of the ESA. The CFSSA issued an Ordinance on ML/TF risk assessment procedure and on the manner of conducting simplified and EDD, which gives detailed instructions to the supervised REs on the RBA expectations in the course of the business relationship or occasional transaction with their clients.

The Financial Inspectorate should adopt Rulebooks or decisions on the specific matters stipulated by the AMLTFL (Art.14(11), and Art.42(1)). The Financial Inspectorate can also adopt sectorial guidelines for the uniform application of the AMLTFL by REs (AMLTFL, Art.88(1)).

The Financial Inspectorate issued respectively an Ordinance on the ML and TF risk assessment procedure for FIs under its supervision and in the way of applying simplified and EDD measures. In addition, the Financial Inspectorate issued a detailed guideline on implementation of the AMLTFL for all supervised REs, including the DNFBPs. In order to assist the REs in implementation of AML/CFT measures, besides the above, Financial Inspectorate also issued the following Sectoral Guidelines: (i) Sectoral Guidelines for Real Estate Agents: the guidelines are published on the website of the MoF and (ii) Sectoral Guidelines on the ML and TF risk assessment procedure and in the way of applying simplified and EDD measures via postal orders: the guidelines are published on the website of the MoF.

The TA can adopt sectorial guidelines for the uniform application of the AMLTFL by REs (AMLTFL, Art.88(1)). The TA respectively issued a detailed guideline for organisers of games of chance on the ML/TF risk assessment procedure and on implementation of the simplified and EDD.

The AMLO should adopt guidelines on the application of certain provisions of the AMLTFL on the basis of the written request of the RE (AMLTFL, Art.141).

The AMLO respectively issued 36 guidelines for REs on application of the national AML/CFT measures. These include: definition of the terms in the AMLTFL; obligations of Res; identification of the BO information; use of the BO Register; detection of the source of funds and other property; application of the EDD; conducting CDD of an existing customer; conducting third party CDD; CDD on legal entities and their representatives; conducting on–going monitoring of customer's financial activities; application of enhanced measures to PEPs; STR and CTR reporting use of collected data; confidentiality of information; data disclosure within a group; record keeping; application of the new technologies; cash restrictions.

*Feedback and Outreach*

The CNB regularly updates its website and publishes Guidance issued by the ESA, as well as FAQs on the effective application of the general AML/CFT requirements. Ad–hoc feedback is provided on occasions of the meetings between the CNB and the professional associations and by responding to individual questions from REs should they have doubts regarding the implementation of their AML/CFT obligations. The CNB reaches out to the supervised FIs on a regular basis, covering a wide range of issues, including ML/TF risk assessment, application of preventative measures, use of new technologies, etc. There were 15 such meetings conducted only in 2019.

The CFSSA publishes on its web site AML/CFT related information. CFSSA holds meetings with REs in relation to implementation of the AML/CFT requirements, as well as other matters when necessary. Outreach is also conducted upon REs' request, where additional explanations and guidance are required. The CFSSA holds regular AML/CFT education activities on an independent basis and in association with other public institutions. So far, the CFSSA, based on questions submitted by supervised FIs, provided clarification on application of specific provisions of the AMLTFL in specific: EDD on customer – public institution; CDD on PEPs; CDD in relationships that are not part of business activities of the RE; identification and verification of a BO; EDD on customer who is not present at identification and verification of identity, etc.

The Financial Inspectorate organised periodic meetings with the supervised FIs with a special focus on the money transfer services sector, which is considered to have a higher ML/TF risk, and significant volume of turnover. Financial Inspectorate holds thematic meetings with representatives of chambers and other DNFBP associations on implementation of the provisions of the AMLTFL.

The TA indicated that the Croatian Gambling Operators Association conducts annual trainings for the representatives of the sector on application of the AMLTFL. In addition, trainings are conducted by the AMLO.

The AMLO is required to provide feedback to REs. This includes specific case–by–case feedback addressed to the RE on the reported STR, and an annual general feedback through publication of typologies, patterns and trends of ML/TF, including anonymised case examples (AMLTFL, Art, 149). In line with these requirements, the AMLO publishes analysis of ML/TF patterns and trends, detected typologies and anonymised case examples in its annual reports. In addition, the AMLO conducted an extensive number of trainings broadly covering all types of REs.

*Weighting and Conclusion*

Croatia has a solid legislative basis supporting and directing the competent authorities in providing the supervised REs with guidance and feedback and conducting outreach. **Croatia is rated C**.

### *Recommendation 35 – Sanctions*

In the 4th round MER of 2013, Croatia was rated PC on R.17. The main deficiencies were the lack of specific sanctions for the failure to comply with some requirements of the AMLTFL and proportionality of sanctions in the financial sector.

***Criterion 35.1 –*** *Implementation of R. 6 on TFS*

Implementation of TFS measures is ensured on the basis of the IRM Law, which provides a range of fines applicable to natural and legal persons for violation of requirements of this Law and regulations enacted on its basis, including the TFS reporting obligation. The range of fines varies depending on the nature of a party violating the requirements (legal person, management of legal person, natural person or self–employed natural person). The sanctions range accordingly minimum from HRK 15 000 to 50 000 (EUR 2 000 – 7 000) for natural persons, and maximum HRK 150 000 – 1 000 000 (EUR 20 000 – 134 000) for legal persons (IRM Law, Art.10(1) and 16). The penalty fines are within the range of the maximum financial sanctions prescribed in the Croatian legislation. Sanctions are considered to be proportionate and dissuasive.

Additionally, any person not acting in accordance with Art. 2(2)(c) and Art. 2(2)(d) of IRM Law may be subject to a prison term from six months to five years (Art. 15(1)). Any person not acting in accordance with Art. 2(2)(a), Art. 2(2)(b), Art. 2(2)(e) and Art. 2(2)(f) may be subject to a prison term of up to three years (Art. 15(2)).

Statutory powers to carry out the supervision of the implementation of the TFS are regulated pursuant to the IRM Law (Art.13) and the Government Decision (N50301–21/21–14–2).

*Implementation of R. 8 on NPOs*

No explicit legal provisions to sanction NPOs in respect to R.8. The sanctions available are relevant to the financial operations of NPO's and would have an indirect application only (Art.45 of the FOA NPO). Within the FOA NPO, the financial supervisor, that has been designated to be the MoJA, has powers to 1) request removal of irregularities within a set deadline, 2) request the return of funds to the state budget if an unlawful use of funds is determined, 3) file criminal charges, 4) submit an indictment for misdemeanour proceedings, and 5) report any suspicion of ML/TF to the AMLO.

The FOA NPO (Art.45) sets out a list of sanctions applicable for non–compliance with the Law. These include a financial penalty of HRK 5 000–200 000 (EUR 670–27 000) for non–compliance with 1) the book–keeping requirements, 2) requirements to register with the NPO Registrar, 3) enable the financial supervisor to perform its supervisory duties, or 4) non–compliance with the decision by the financial supervisor to remediate irregularities or deficiencies.

*Preventative measures R. 9–23*

Chapter VII of the AMLTFL sets out the sanctions in the form of fines for violations of certain obligations set out in this Law. The Council for Misdemeanour Proceedings (under the Financial Inspectorate and established within the MoJA) is the only body with authority to impose monetary fines under the AMLTFL. All supervisory authorities have the legal powers to impose sanctions directly on REs under Art.233 and 228 of the Misdemeanour Act.

Furthermore, Supervisory authorities, when determining violations of the provisions of the AMLTFL and by–laws, are authorised to apply the following types of sanctions: written warning; fine; temporary prohibition of certain business activities by the REs or their management; prohibition of carrying out certain duties, activities or tasks by the REs; revocation of licence.

The AMLTFL (Art.150(1)) lists types of misdemeanours for which a financial penalty of HRK 35 000 to HRK 1 mln. (EUR 4 700 to EUR 134 000) may be imposed. The list includes 65 misdemeanours that include requirements for R.9–23 (subject to any deficiencies identified above).

Where the RE is an authorised exchange office, legal or natural person engaged in dealing in precious metals, or art trader, the financial penalty available if the firm fails to identify or verify the customer identity is lower, HRK 10 000 to HRK 350 000 (EUR 1 300 to EUR 47 000).

Art.150(6) does allow for the financial penalty to be imposed on double the amount of the pecuniary gain or be increased to HRK 7 500 000 (EUR 1mln.), in respect of the most severe misdemeanours. Where the RE is a credit or financial institution, the financial penalty may be increased further to HRK 38 000 000 (EUR 5mln.) or 10% of the total annual income according to the latest available financial statements.

However, there is no definition of which misdemeanours are considered to be more severe. Furthermore, the sanctions applicable to natural persons acting as lawyers, notaries, auditors, accountants and tax advisors cannot be greater than HRK 450 000 (EUR 60 000).

Art.151(1) of the Law lists a further 21 misdemeanours to which a financial penalty of HRK 25 000 to HRK 800 000 (EUR 33 000 to EUR 106 000) applies.

The AMLFTL has separate financial penalty provisions in respect to payment institution transactions ranging from HRK 50 000 to HRK 1 mln. ( EUR 6 700 to EUR 134 000)

Furthermore, the sanctions applicable to lawyers, notaries, auditors, accountants and tax advisors cannot be greater than HRK 350 000 (EUR 47 000) for misdemeanours prescribed in Art.153.

There are a series of other misdemeanours listed in Art.153 referring to failings of requirements or specifically referring to a type of RE. The financial penalty for these ranges from HRK 5 000 to HRK 350 000 (EUR 670 to EUR 47 000).

***Criterion 35.2 –*** *Implementation of R. 6 on TFS*

Fines provided under the IRM Law can be applied to legal persons, members of the management board or another responsible person in the legal person, natural person or self–employed natural person (IRM Law, Art. 16).

*Implementation of R. 8 on NPOs*

As per c.35.1, there are no explicit legal provisions to sanction NPOs in respect to R.8. The sanctions available are relevant to the financial operations of NPO's and would have an indirect application only. The FOA NPO (Art.45) provides for sanctions applicable specifically to natural persons. However, these sanctions do cover the full scope of key functions as required by the FATF Standards. These are limited to: 1) financial penalty of HRK 5 000–200 000 ( EUR 670 – 27 000) to the legal representative of an NPO for non–compliance with double–entry requirements; 2) financial penalty of HRK 1 000 – 10 000 (EUR 133–1 330) to the legal representative of an NPO for non–compliance with simple–entry booking requirements; and 3) financial penalty of HRK 10 000 – 50 000 (EUR 1 330 – 6 700) to the head of a state administration body that is of a local and regional self–government unit, for the approval of a payment to an NPO that has not been registered in the Register of NPOs.

*Preventative measures R. 9–23*

Fines provided under the AMLTFL can be applied to legal person, member of the management board or another responsible person (AMLTFL, Art. 150–153).

Definition of "Senior management of the RE" clarifies that "it does not have to be, in all cases, a member of the management board or another managerial body" (AMLTFL, Art. 4(47)).

*Weighting and Conclusion*

Croatia has a very wide range of sanctions, depending on the seriousness of the breach, the type of RE, and in respect to natural and legal persons. Whilst the sanctions appear to have been increased since 2019, a large number of these are relatively low amounts that put into question is they can be dissuasive. Sanctions in respect to NPOs are indirect and do not cover the full scope of the FATF Standards. Therefore, it cannot be considered that Croatia has a range of proportionate and dissuasive sanctions in place. **R.35 is rated PC**.

### *Recommendation 36 – International instruments*

In the 4th round MER of 2013, Croatia was rated PC on both R.35 and SRI. The Croatian authorities were criticised for failing to comply with the requirements to implement the Vienna, the Palermo and the UN conventions.

***Criterion 36.1*** – Croatia is party to all four conventions listed in the Standards. Croatia notified succession to the *Vienna* Convention, as former Yugoslavia ratified this in 1991, ratified the Palermo Convention in 2002, United Nations Convention against Corruption (Merida Convention) in 2005, and the Terrorist Financing Convention in 2003. As concerns the Conventions listed in the Annex of the TF Convention, Croatia did not yet ratify the 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, as well as the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.

It should be noted that in 2008 Croatia became a party to, *inter alia*, the 2005 Warsaw Convention of the Council of Europe.

***Criterion 36.2*** – Croatia has broadly implemented the provisions of the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption and the International Convention for the Suppression of the Financing of Terrorism. However, deficiencies are identified with regard to the implementation of provisions of: (i) the Palermo Convention – namely Art.6 is not fully implemented since criminalisation of ML offence does not cover all elements of self–laundering; (ii) the Merida Convention – namely Art.14 is not fully implemented as requires comprehensive implementation of preventive measures, Art. 23 is not fully implemented due to the deficiencies same as to Palermo Convention, Art. 26 is not fully implemented since the sanctions for criminal liability of legal persons are not dissuasive, and Art. 31 is not fully implemented since management of seized legal persons is not envisaged in Croatian legislation; (iii) the TF Convention – namely Art.2 is not fully implemented since the acts of placing and discharging an explosive or other lethal device which constitutes an offence as defined in the 1997 International Convention for the Suppression of Terrorist Bombings are not criminalised under the Croatian CC. Furthermore, no definition of funds or other assets is provided in the criminal legislation, and financing of travel for the purpose of preparation of a terrorist act is not considered as a criminal offence. While deficiencies are numerous, these are considered to be moderate.

*Weighting and Conclusion*

Croatia ratified all four conventions. Croatia has broadly implemented the provisions of the Vienna Convention, the Palermo Convention, the Merida Convention and the International Convention for the Suppression of the Financing of Terrorism, but moderate gaps remain. **R.36 is rated PC.**

### *Recommendation 37 – Mutual legal assistance*

In the 4th round MER of 2013, Croatia was rated LC both on R.36 and SRV. Deficiencies were related mostly to the impact that the gaps in the national framework would have on international co–operation. These, among others, included the impact of deficiencies in criminalisation of the ML, in the confiscation regime, and in application of provisional measures.

***Criterion 37.1*** – The legal framework of Croatia for providing MLA is comprised of a network of international treaties, conventions, EU legislative framework implemented in the JCCMEUL with the EU Member States, as well as Mutual Legal Assistance in Criminal Matters Law (MLA Law) to complement the toolkit for international co–operation where there are no other mechanisms available. This legal basis allows for providing a wide range of MLA with respect to investigation and prosecution of ML, TF and predicate offences when requested by foreign jurisdictions. MLA requests should be executed within the deadlines indicated in the request (MLA Law, Art.10(2), JCCMEUL, Art.42k).

***Criterion 37.2*** – The MoJA is the central authority responsible for transmission of foreign MLA requests to/from domestic judicial authorities (MLA Law, Art.6). For the purposes of co–operation within the EU Member State, the MoJA is the central authority for establishing contacts and judicial co–operation (JCCMEUL, Art.5(5)).

Timely execution of MLA requests is ensured through the provisions of the MLA Law (Art.10(2) and JCCMEUL (Art.42k). Respectively, requests of a non–EU Member State shall be executed without delay, taking into account procedural deadlines, as well as other specially determined deadlines explained in the request, and when dealing with the EU Member State request – deadlines provided for taking of evidentiary action in domestic law, giving the same priority as in a comparable domestic case, always respecting the deadlines provided by the JCCMEUL. If the request of a foreign judicial authority may not be executed, in full or in part, the Croatian domestic judicial authority is obliged to inform the foreign judicial authority of this effect without delay, indicating the conditions under which such request may be executed (MLA, Art.10, and JCCMEUL, Art.42k(5–6)). Further than this there is no regulation on the prioritisation or timeframes for execution of requests which affects co–operation, in particular with non–EU Member States.

In order to ensure monitoring of the progress, the MoJA uses International Legal Assistance System for electronic case management. The International Legal Assistance System allows to process the MLA case files, categorising the requests (based on the criminal offence is in question, requesting jurisdiction, type of MLA requested, etc.), prioritising these, and assigning a responsible person.

***Criterion 37.3*** – Aside from the contradiction in the treatment of requests concerning fiscal offences (see c.37.4(a)), the Croatian legislation does not provide any prohibitions and/or restrictive conditions on MLA.

***Criterion 37.4*** – (a) Croatia can refuse MLA request if it concerns a fiscal offence (MLA Law, Art. 12 (1–2)). At the same time, paragraph 3 of the same Art. makes a reference to the inability to refuse the MLA request solely on the ground that it relates to fiscal offence. This contradiction raises the issue of the consistency of treatment of the relevant request.

At the same time the JCCMEUL (Art.47(1(3)), which is applied to co–operation within the EU framework, stipulates that for fiscal offences, the execution of an order may not be refused merely because domestic law does not prescribe the same type of tax or fee or does not contain the same provisions on taxes, duties, customs and currency exchange as the law of the issuing State.

(b) Neither the MLA Law (Art.12(1) and 13(1)) nor JCCMEUL (Art.47(1–2)) includes secrecy or confidentiality matters in their mandatory or discretionary grounds for refusal. See also under R.9 as far as FIs are concerned.

***Criterion 37.5*** – Under the MLA Law, the confidentiality obligation for the MoJA and the domestic judicial authorities are limited to keeping confidential the request for mutual assistance, and its substance only to circumstances when a foreign judicial authority requests so (Art.21(1)). The JCCMEUL stipulates that on the basis of the information and special requirements indicated in the EIO for the purpose of ensuring secrecy and in accordance with its national law, the competent judicial authority shall guarantee the confidentiality of the facts and content of the EIO, except to the extent necessary (Art.42s(1)). In addition, in the circumstances where the bilateral or multilateral international agreements are in place, the respective confidentiality requirements will be followed.

***Criterion 37.6*** – Dual criminality is not a prerequisite for execution of MLA requests which does not involve coercive measures. This can be inferred from the absence of dual criminality conditions in the provisions of the MLA Law (Art.1(2), Art.4, Art.5, Art.12 and Art.13). Under the JCCMEUL, dealing with co–operation among the EU Member States, dual criminality is only required for conducting coercive actions, unless this falls under the categories of a specified list of offences (Art.47(1(3)).

***Criterion 37.7*** – As indicated in c.37.6, dual criminality is a precondition to coercive actions requests exchanged with EU Member States only. However, the principle of dual criminality is satisfied regardless of whether both countries place the offence within the same category of the offence or they nominate the offence by the same terminology. The only requirement is that both countries criminalise the conduct underlying the offence.

***Criterion 37.8*** – Competent authorities may use all powers available for the investigation of crimes domestically in response to requests for mutual legal assistance. This includes:

(a) all the specific powers required under R.31 relating to the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions or other natural or legal persons, and the taking of witness statements (MLA Law, Art.3, 25, 26, 28, 50 and 81; CPC, Art.332 and, JCCMEUL, Art. 42e, 42h and 132); and

(b) A broad range of other powers and investigative techniques, including the application of compulsory measures and use of special evidence gathering techniques available to the LEAs and the Court for the purposes of investigation and prosecution of ML/TF and other predicate offences within the MLA request (JCCMEUL, Art.42aa, 42am, 42ao, 42ap).

However, Croatia did not demonstrate how the investigative techniques as required under R.31 can be used in the framework of direct co–operation between foreign judicial or LEAs and domestic counterparts. Deficiencies identified under R.31 apply.

*Weighting and Conclusion*

Croatia meets most of the criteria, providing for a wide range of MLA in relation to investigations, prosecutions and related proceedings involving FT, ML and associated predicate offences. However, the grounds for refusing MLA when dealing with a fiscal offence contradict requirements of the Recommendation. In addition, among other minor deficiencies, the existing legislation does not contain any prioritisation requirements when dealing with ML/TF international co–operation. **R.37 is rated LC.**

### *Recommendation 38 – Mutual legal assistance: freezing and confiscation*

In the 4th round MER of 2013, R.38 was not reassessed due to the requirement of the MONEYVAL's 4th round Rules of Procedure. The rating LC in the 3rd round MER (2008) was maintained. The deficiency was that due to absence of statistics, it was impossible to establish the effectiveness and timeliness of MLA on freezing, seizure or confiscation; Croatia has not considered establishing an asset forfeiture fund to be used for the LEAs, health, education or other appropriate purposes; no arrangements in place for coordinating seizure or confiscating actions and sharing of confiscated assets with other countries.

***Criterion 38.1*** – The Croatian legal framework described under R.37 also applies to MLA in the field of identification, freezing, seizing and confiscation of ML/TF proceeds and proceeds from predicate offences.

As concerns the MLA Law, this regulates measures related to identification (Art.3 and Art.50) and a temporary seizure of laundered property, proceeds, or their corresponding value, and instrumentalities used to commit a crime (Art.29(1–2)). These provisions apply to any offence under the Croatian legislation. The request should be executed within the indicated deadlines (Art.10(2)). When concerns the ML/TF and some other predicate offences, the MLA Law requires to take expeditious actions (Art.20). Nevertheless, the legislator does not specify whether the instrumentalities would also include the ones that are intended for use. The powers to confiscate these objects are not specified either.

Pursuant to the JCCMEUL, when receiving a decision of a foreign judicial body on confiscation of property or objects, the Croatian court will recognise it without delay, and this will be executed in accordance with domestic law (Art.64). Respectively, provisions of the CC will apply, as detailed in R.4.

Deficiencies indicated under R.4 regarding shortcomings in the domestic confiscation system have an impact on this criterion.

***Criterion 38.2*** – There are no explicit provisions that would demonstrate how the non–conviction based provisions would apply under the legal framework of Croatia. Nevertheless, the MLA Law stipulated that when there are no special procedural rules provided on the MLA, the provisions of the CPC will apply (Art.81). The CPC respectively stipulates that property can be confiscated when the criminal proceedings do not end with a verdict finding the defendant guilty (Art.556(1)). Confiscation measures can be applied in the circumstances when the person against whom criminal proceedings have been instituted are permanently inaccessible to criminal proceedings, only when the proceeds amount to at least HRK 60 000 (EUR 8 000). In these circumstances, the State Attorney shall request the court to establish that the person has committed an unlawful act and that he has obtained material gain, and that the property benefit should be confiscated from that person or the person to whom it is transferred (Art.560b(1–2)). This can also be done when the perpetrator is not available by reason of death (Art.560f). These provisions do not detail whether this would apply to confiscation of the property as specified under c.38.1 and whether the confiscation would be possible when the person is absent by reason of flight, absence or if the perpetrator is unknown.

The EU Regulation 2018/1805 on the mutual recognition of freezing orders and confiscation orders applies to all confiscation orders, including non–conviction based confiscation (Point 32 of the Preamble). The Criminal Procedure Code shall apply mutatis mutandis to all matters which

are not governed by the JCCMEUL (Art.132). Co–operation with Ireland and Denmark is governed by Chapter V of the JCCMEUL.

***Criterion 38.3*** – (a) The Asset Recovery Office (in the PNUSKOK) and the ARO network can also play a coordination role. Furthermore, Croatia is party to the CARIN network. As far as coordinating investigations and the actions of judicial authorities in relation to seizure and confiscation actions, both EUROPOL and EUROJUST also provide coordination mechanisms. Croatia does not have arrangements in place for coordinating seizure and confiscation actions with other countries on the basis of bilateral and multilateral agreements.

(b) Croatia has a domestic mechanism for managing and disposing of seized and confiscated property. This is regulated under the EU Regulation on the conditions and methods of management of the temporary seized property in criminal proceedings and the SPM Law. The responsible authority for the management of property is the MPPCSA. Croatia, nevertheless, did not demonstrate how would be the managements of property applied within the context of MLA. Under Art.71 of the JCCMEUL, the Croatian authorities are able to dispose of confiscated property applied within the context of MLA with EU members. No information has been provided on disposal of assets with non–EU countries. Deficiencies under R.4, apply.

***Criterion 38.4*** – Croatia has a domestic mechanism to share confiscated property with EU Member States, in the amount of 50% of the collected amount assigned to the issuing country if the collected amount exceeds EUR 10 000 (JCCMEUL, Art.71(1)). However, Croatia has not demonstrated on which basis it would be able to share confiscated property with non–EU countries, especially when this would be a result of co–ordinated law enforcement action. Nevertheless, as a party to the UNCAC or CETS 198, Croatia will be bound by the particular provisions of the said Conventions with regard to sharing of assets. However, these are only limited instances and do not suggest meeting the requirements of the FATF Standards in a broad sense.

*Weighting and Conclusion*

Croatia has ability to provide MLA concerning identification, freezing, seizure and confiscation measures. However, moderate shortcomings remain, in particular, when dealing with non–EU Member States. There are also no clear procedures for providing co–operation on the basis of non–conviction based confiscation, a mechanism for managing and sharing of confiscated property. The asset sharing mechanisms proscribed by UNCAC or CETS 198 apply in limited cases only. **R.38 is rated PC.**

### *Recommendation 39 – Extradition*

In the 4th round MER of 2013, R.39 was not reassessed due to the requirement of the MONEYVAL's 4th round Rules of Procedure. The rating LC in the 3rd round MER (2008) was maintained. The deficiency was that because of the shortcomings in TF criminalisation, the requirement of dual criminality for extradition would mean that not all kinds of terrorist financing offences would be extraditable.

***Criterion 39.1*** – In Croatia, extradition is governed by national legislation, bilateral and multilateral agreements, and ratified conventions. At the national level the regulatory framework is set through two main legal acts: JCCMEU (Chapter II) that implements the European arrest warrant and the surrender procedures between the EU Member States, and MLA Law (Chapter III) that provides a regulatory framework for extradition with non–EU member jurisdictions,

where there are also no bilateral or multilateral agreements in place. Croatia ratified the Council of Europe European Convention on Extradition and two additional Protocols, but not its 3rd and 4th additional protocols. With regards to extradition within the EU Member States, the legislative provisions require taking urgent action (JCCMEUL, Art.32). There is no similar provision envisaged under the MLA Law to ensure urgent extradition when co–operating with non–EU Member States.

(a) ML and TF are extraditable offences (JCCMEUL, Art.10 and 17, MLA Law, Art.34).

(b) In order to ensure monitoring of the progress, the MoJA uses International Legal Assistance System for electronic case management. The International Legal Assistance System allows to process the MLA case files, categorising the requests (based on the criminal offence is in question, requesting jurisdiction, type of MLA requested, etc.), prioritising these, and assigning a responsible person.

(c) The conditions for the non–execution of requests as defined by the JCCMEUL (Art.20–21) and the MLA Law (Art.35) do not appear unreasonable or unduly restrictive.

***Criterion 39.2*** – (a) It is prohibited to extradite Croatian nationals to another state, except in the execution of a decision on extradition or surrender made in accordance with an international treaty or the acquis Communautaire of the European Union (Constitution, Art.9), which is implemented through the JCCMEUL.

Among the agreements concluded by Croatia with foreign jurisdictions, extradition of nationals for ML is envisaged with Bosnia and Herzegovina, Montenegro, and Macedonia. Croatia has not concluded similar agreements for TF.

(b) If an EAW has been issued, under special conditions, when the citizen or resident of Croatia agrees to serve the sentence in Croatia, the request will be postponed, the Croatian court should issue a decision on taking over the execution of a foreign sanction, and when it is final, refuse recognition of the EAW. The court shall request documentation from the issuing state and set an appropriate deadline, which may not be longer than 15 working days for its delivery (JCCMEUL, Art.22(4)). Croatia can extradite its citizens in line with provisions of JCCMEUL (Art.29).

Where there are no agreements in place and does not concern the EU Member States, in accordance with the MLA Law, extradition cannot be granted if it concerns the citizen of Croatia (Art.32(1)) and the citizenship of Croatia is a ground for refusal (Art.35(1(1)). When extradition is not allowed, the domestic judicial authority may take over carrying out criminal proceedings for a criminal offence committed abroad (MLA, Art.62). While the provision is worded as a discretionary measure, the principle of application of the Croatia criminal legislation to offences committed by the citizens abroad, as set out under the CC (Art.14 and 16), sufficiently overcome this flexibility. Relevant requests of foreign judicial authority to undertake criminal prosecution against a Croatian national or domiciled person for an offence committed abroad are dealt with as if committed in Croatia (MLA, Art.65). Respectively, the domestic procedural deadlines would apply.

**Criterion *39.3*** – Both the JCCMEUL (Art.20) and MLA Law (Art.34(1)) require dual criminality for extradition.

Pursuant to JCCMEUL, when a foreign request concerns the list of offences provided under Art. 10, which include ML and a number of predicate offences, but not TF, Croatia need not check the double criminality. Otherwise, the requirement of double criminality should be considered

satisfied provided that it contains essential features of the offence, regardless of the legal description and legal qualification of the offence specified in the foreign request (Art.20(1)).

Pursuant to MLA Law requires the extradition to be provided if the domestic law incorporates corresponding essential features of the relevant foreign offences (Art.34(1)).

***Criterion 39.4*** – Simplified extradition with the written consent of the person to be extradited is envisaged in Croatian legislation both for the request from EU Member States (JCCMEUL, Art.28) and non–EU Member States (MLA Law, Art.54).

*Weighting and Conclusion*

Croatia has a mechanism for extradition procedures. However, some gaps identified in criminalisation of the TF offence may impact the scope of application of these measures. **R.39 is rated LC.**

### *Recommendation 40 – Other forms of international co–operation*

In the 4th round MER of 2013, Croatia was rated Largely compliant on R.40. The deficiencies related to absence in the AMLTFL of provisions dealing with the predicate offence co–operation, as well as the lack of comprehensive statistics on international co–operation.

*General Principles*

***Criterion 40.1*** – All competent authorities are able to provide the widest range of international co–operation in relation to ML, associated predicate offences and TF, on a timely basis, spontaneously and upon request (AMLTFL, Art.90–93, Art.127–130, JCCMEUL, Art.3(4), 6–8 and 10, other sectorial legislation). Co–operation with EU and non–EU Member States is conducted on the basis of conventions, bilateral and multilateral agreements or on the basis of reciprocity. Croatia also co–operates through mechanisms provided by the Egmont Group, EUROPOL, EUROJUST, INTERPOL and others.

***Criterion 40.2***

(a) Competent authorities have a legal basis for providing co–operation – see c.40.1 above;

(b) Competent authorities are not prevented from using the most efficient means possible for providing the widest range of assistance;

(c) The AMLO uses secure communication channels (FIU.net, EGMONT Secure Web and encrypted e–mails) in the international data exchange with a foreign FIU (AMLTFL, Art.136)

CNB – does not have clear and secure mechanisms that will allow the transmission and execution of requests. However, they can enter into multilateral agreements enabling exchange of information through designated contact points (Directive (EU) 2015/849 (Art.57a(2)), (Credit Institutions Law, Art.212).

Financial Inspectorate does not have established secure channels of communication with its foreign counterparts.

The TA communicates with EU Member States via EU COM (DG TAXUD) secure CCN/CSI (Common Communication Network/Common Systems Interface), and with third countries via certified or priority mail. However, there is no explanation of what is “certified” or “priority” mail means, nor of who are the counterparts with which Croatia exchanges information through this

mean. In addition, the TA does not have a secure and clear channel to exchange information with its foreign counterparts in its capacity as casino supervisor.

The CA uses the European Anti–Fraud Office Customs Information System (CIS) and the Naples II Convention, which ensures secure exchange of information with its EU counterparts. With non–EU counterparts, it exchanges information in a formal way based on bilateral agreements. Data from cash seizures are inserted into the designated secure World Custom's Organisation platform CEN–comm (Customs Enforcement Network Communication Network).

The Police – uses the INTERPOL (I–24/7), EUROPOL (SIENA) and SIS (SIRENE) mechanisms, as well as, the framework of the Swedish initiative, the liaison officers abroad and foreign police liaison officers in Croatia. Police can partially use the SIS2 system: as they are not full Schengen members, they cannot enter alerts concerning bans on entering Schengen areas but can deal with other alert circumstances.

(d) The AMLO follows the Egmont Principles for the prioritisation or timely execution of requests. The Police, the CNB and the TA, when co–operating on tax matters, also have clear procedures on prioritisation of requests from the foreign counterparts. However, there are no formal procedures for other competent authorities (Financial Inspectorate, the CFSSA and the TA when acting as supervisor) to apply prioritisation and timely execution of the request, rather it is done on a case–by–case basis.

(e) The AMLO, the CNB, the Financial Inspectorate, the TA when acting on tax matters, the CA, the Police and the CFSSA have clear procedures for safeguarding the information received from foreign counterparts (AMLTFL, Art.128 (3–4) and 143; CNB Law, Art. 31(2); Financial Inspectorate Law, Art. 36; General Tax Law, Art. 8; CA Law, Art.24; PDPL, Art.23(3)). However, TA as a supervisory body does not have processes for safeguarding the information received from foreign supervisory counterparts.

***Criterion 40.3*** – Where necessary, all the competent authorities except the TA in its capacity as supervisor are empowered to sign and have a network of bilateral and multilateral agreements, MoUs and protocols to facilitate international co–operation with a range of foreign counterparts (AMLTFL, Art.127(7–8); Credit Institutions Law, Art.212(1) and 208(1); Leasing Act, Art.57(9) and 58(5); Factoring Act, Art.44(9) and 45(5); Capital Market Law, Art.509(9); Insurance Law, Art.397(15); Law on the Police Duties and Powers, Art.10).

***Criterion 40.4*** – The AMLO, and the Police, TA and CA, when co–operating with EU Member States, provide timely feedback upon request on the use of the requested information (AMLCFT Art. 134(2), EG Principles Section 19, JCCMEUL, Art.11(6)). Regarding non–EU Member States, the Police and the CA informed that it is not a standard procedure to send feedback regarding received information and use of the obtained information, but this information can be provided on a case–by–case basis. While no explicit provisions to regulate this, the CNB and CFSSA confirmed to have ability to provide such feedback when requested within the scope of the international agreements and general regulatory framework on co–operation. No practice was observed regarding Financial Inspectorate and TA on providing feedback when co–operating with non–EU Member States.

***Criterion 40.5*** – (a) Competent authorities do not refuse EU Member States' requests involving fiscal matters (AMLTFL, Art.90(3), 92, 127 and 129; JCCMEUL, Art.12). Co–operation with non–EU Member States is conducted on the basis of MoUs, which do not contain unreasonable or unduly restrictive conditions (e.g., Agreement between Croatian and Serbian government on police co–operation from May 2009, Agreement between Croatian government and Council of

Ministers of Bosnia and Herzegovina on police co–operation and fight against cross–border criminality, signed in September 2010, Agreement between Croatian and North Macedonian government on police co–operation, signed in May 2012).

(b) Competent authorities do not refuse EU Member States' requests constituting secrecy or confidentiality, except if it can have a negative impact on the investigation conducted on the national level (AMLTFL, Art.77, 90(3), 92 and 129). This refers to co–operation with both EU and non–EU Member States.

(c) Competent authorities do not refuse EU Member States' requests, unless the exchange of the requested information would interfere with that inquiry, investigation or proceeding (AMLTFL, Art.90(3), 92 and 129, JCCMEUL, Art.12(2)). As for co–operation with non–EU Member States, some MoUs signed by the CFSSA include the possibility to deny a request if a criminal proceeding based upon the same fact and against the same persons has been initiated in the State of the requested Authority. This is contradictory with the FATF Standards.

(d) Competent authorities do not refuse co–operation with EU Member States due to the different nature or status of the competent authority requesting the exchange of information (AMLTFL, Art.90(3), 92 and 127(3); JCCMEUL, Art.1 and 3(3)). Co–operation with non–EU Member States is conducted on the basis of MoUs, which do not contain unreasonable or unduly restrictive conditions.

***Criterion 40.6*** – The current legislation ensures that the information provided and received by the AMLO, the Police, TA and the CA, the CNB and the CFSSA is used only for the purposes and to the extent indicated in the request. Any additional actions, including the use of the relevant data by the previously unspecified authorities, require an additional confirmation by the disseminating authority (AMLTFL, Art.127(5(2)), 128(3–4)). This applies to co–operation with both EU (JCCMEUL, Art.11) and non–EU Member States (AMLTFL, Art.92, Credit Institutions Act, Art.209(2)3, e.g., Agreement between the Croatian government and Council of Ministers of Bosnia and Herzegovina on police co–operation and fight against cross–border criminality, signed in September 2010, Art.23). Nevertheless, this requirement does not apply to the Financial Inspectorate or the TA acting in its capacity of casino supervisor.

***Criterion 40.7*** – Competent authorities maintain appropriate confidentiality of international requests, consistent with the existing privacy and data protection requirements, protecting the information obtained the same manner as they protect domestic data (AMLTFL, Art.11, 90(3)d, 92(1), 127(5), 128(4), JCCMEUL, Art.11(1–2), Act on the CNB, Art.53(1)). However, none of them has the power to refuse providing information if the requesting foreign authority cannot secure the confidentiality of this information.

***Criterion 40.8*** – Most of the competent authorities are able to conduct inquiries on behalf of a foreign counterpart, providing them with all available information as if such inquiries were carried domestically (AMLTFL, Art.90(2)), 113, 116, and 127(1), JCCMEUL, Art.5(2))). However, the TA has no mechanism to collect information on behalf of foreign counterparts in its capacity as AML/CFT supervisor of games of chance.

*Exchange of Information between FIUs*

***Criterion 40.9*** – The AMLO has sound legal basis for providing co–operation on ML/TF and associate predicate offence (AMLTFL, Art.127, 129, and 130).

***Criterion 40.10*** – Upon request and whenever possible, the AMLO should provide feedback to the foreign FIUs on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided (AMLTFL, Art.134(2), EG Principles Section 19).

***Criterion 40.11*** – (a) AMLO shall exchange with the foreign FIU all information, data and documents needed for detecting and preventing ML/TF, that it collects or maintains (AMLTFL, Art.129 (1)). This can include any information, data or document obtained directly or indirectly.

(b) On the basis of reciprocity, the AMLO can exchange information with foreign FIUs and other and other foreign authorities and international organisations competent for AML/CFT, collecting additional data from REs and other competent authorities (AMLTFL, Art.127(6)).

*Exchange of Information between financial supervisors*

***Criterion 40.12*** – Croatia has a legal basis enabling Supervisors to co–operate with foreign counterparts from the EU Member States, regardless of their nature or status (AMLTFL, Art.90). However, co–operation with foreign counterparts from non–EU Member States is possible only for the purposes underlined in the request if the co–operation agreement has been concluded, and the confidentiality requirements are met (AMLTFL, Art.92).

***Criterion 40.13*** – Financial supervisors shall, within the scope of their authority, co–operate and exchange information with foreign counterparts from EU Member States (AMLTFL, Art.90(1)). In addition, they are empowered to collect information on behalf of the competent foreign authority requesting the assistance and the exchange of the information collected (AMLTFL Art. 90(2)). Exchange of information with the foreign counterparts from non–EU Member States is based on the signed agreements.

***Criterion 40.14*** – The AMLTFL provides general powers to CNB, CFSSA and the Financial Inspectorate to co–operate and exchange information with counterparts from EU Member States (AMLTFL, Art.90(1)). It does not limit, but neither specify the type of information that can be exchanged.

Exchange of information between the CNB, CFSSA and the Financial Inspectorate and counterparts' competent authorities from third countries, is subject to signed agreements (AMLTFL, Art.92(1)).

(a) Regulatory information in the Republic of Croatia is publicly available and can be provided without restrictions.

(b)-(c) Several sectorial laws specify the framework of co–operation with foreign counterparts for the CNB and the CFSSA, indicating the ability to exchange "information" or "confidential information" (Credit Institutions Act, Art.208(1), 209(1)) and 212(1) and (2); PSL, Art.150(4–1)); Electronic Money Act, Art.79(1), Art.84(1); Law on pension insurance companies, Art.199(1); Law on open investment funds with public officers, Art.387(1); Law on alternative investment funds, Art.273(1), Law on voluntary pension funds; Art.308a(1); Insurance Law, Art.397(4); Leasing Law, Art.106(3–2); Law on Capital Markets, Art.401(1)). However, the specific meaning of these terms remains unclear. No specific legal framework for co–operation with foreign supervisory authorities is foreseen for the Financial Inspectorate, except the provision stated in the AMLTFL.

***Criterion 40.15*** – The CNB, Financial Inspectorate, CFSSA and TA are able to collect information on behalf of their foreign counterparts from EU Member States (AMLTFL, Art.90(2) and 86(2)). The CNB, CFSSA and Financial Inspectorate co–operate with non–EU Member States through

bilateral and multilateral agreements, which provide a wide scope of assistance for competent authorities to conduct inquiries on behalf of their counterparts and exchange relevant information. No such provision is prescribed for the TA in its capacity as supervisor.

In addition, there is no information provided on the ability of the foreign counterparts to conduct inquires themselves in the Republic of Croatia in order to facilitate effective group supervision.

***Criterion 40.16*** – The CNB, Financial Inspectorate, CFSSA and TA shall keep the received information confidential, may use it only for the purpose for which it was given and communicate it only with the express consent of the body providing that information (Credit Institutions Act, Art.209(2)(3) and (3)(3); Electronic Money Act, Art.94(4); Law on Payment services, Art.151(4); Law on pension insurance companies, Art.198c(3); Insurance Law, Art.397(8)(3); Law on alternative investment funds, Art.281(3); Law on open investment funds with a public officer, Art.389(3); Factoring Act, Art.100(4); Law on voluntary pension funds, Art.309(4); Capital Market Law, Art.401(3); Leasing Law, Art.108(4); Insurance Law, Art.397(8)(3)).

However, the legal framework does not contain any provisions mentioning the obligation of communicating the information only with the express consent of the body providing that information and does not envisage cases where the requesting financial supervisor is under a legal obligation to disclose or report the information.

*Exchange of Information between LEAs*

***Criterion 40.17*** – LEAs can exchange domestically available information with foreign counterparts for both intelligence and investigation purposes related to all crimes, including through channels of international organisations such as Interpol and Europol, as well as bilateral agreements. This includes identification and tracing of assets (JCCMEUL, EU Regulation 1889/2005).

***Criterion 40.18*** – The Police, TA and CA can use the powers available domestically to conduct inquiries and obtain information on behalf of their EU counterparts, based on the agreements concluded as part of the Interpol, Europol and Eurojust co–operation (JCCMEUL, Art.2 and 5). As for non–EU counterparts, the co–operation is conducted according to mutually agreed conditions reflected in the MoU (Ex. Agreement between Croatian and Moldovan government on co–operation in the fight against organised crime, illegal drugs trafficking, terrorism and other serious crime, 2006).

***Criterion 40.19*** – Croatia is able to form a joint investigative team in accordance with an international agreement or on the basis of an individual case for the criminal offences within the scope of USKOK (USKOK Law, Art.17; PDPL, Art.22 (2002/465/JHA) (OJ L 162, 20.6.2002)).

As concerns non–EU Member States, co–operation is conducted according to mutually agreed conditions reflected in the MoU (ex. Agreement between Croatian government and Council of Ministers of Bosnia and Herzegovina on police co–operation and fight against cross–border criminality, 2010)

***Criterion 40.20*** – The AMLO can use secure communication channels via a foreign FIU for the purposes of asking and receiving data, information and documentation from/to another foreign authority (AMLTFL, Art.137).

The JCCMEUL provides for the ability of the Police, TA and CA to exchange information indirectly with non–counterpart authorities of EU member–states.

The CA indicated the possibility of diagonal co–operation via LEAs.

*Weighting and Conclusion*

Croatia can provide a wide range of international co–operation via informal means (e.g., through the AMLO, LEAs and financial supervisors). However, some deficiencies remain: i) the TA has no legal basis nor secure channels to communicate in the capacity of a supervisor over the game of chance; ii) the legal framework for the Financial Inspectorate provides for international co–operation with EU Member States only; iii) none of the competent authorities can refuse data provision if the requesting authority cannot protect the information effectively, iv) supervisors (but the CNB) do not have mechanisms for prioritising international requests, v) there is no provision mentioning the obligation of supervisors to communicate the information only with the express consent of the body providing that information. Neither the CNB nor the CFSSA provisions envisage cases where the requesting financial supervisor is under a legal obligation to disclose or report the information; vi) some of the MoUs signed by the CFSSA contain a provision allowing to refuse a request if a criminal proceeding has been initiated in the State of the requested authority; vii) the provisions for information exchange of the CNB and the CFSSA do not specify whether the term "information" includes prudential and AML/CFT information. **R.40 is rated PC.**

## Summary of Technical Compliance – Deficiencies

## ANNEX TABLE 1. COMPLIANCE WITH FATF RECOMMENDATIONS

| Recommendations | Rating | Factor(s) underlying the rating |
|---|---|---|
| 1. Assessing risks & applying a risk–based approach | **PC** | • There are some issues with how the assessment of ML/TF risks were conducted:<br>- lack of quantitative data used when assessing ML/TF;<br>- inflexible and inadequate manner of application of risk assessment methodology, e.g., when assessing and scoring the residual risks, and grouping the DNFBPs with different profiles.<br>- Vulnerabilities in relation to TF are treated identically to ML across each sector, which does not appear to align with the country's context.<br>- Identification and assessment of the TF risks is not sufficient.<br>- ML/TF risks in some areas were not appropriately explored (see IO.1).<br>• The 2020 Action plan is non–contentious and does not tackle the fundamental issues raised across the two risk assessments, such as lack of successful ML/TF prosecutions, lack of measures regarding detection and confiscation, the need for further training of the judiciary, law enforcement and investigators, inability to secure an adequate number of personnel in the Financial Inspectorate, addressing barriers to recruitment of financial investigators, etc.<br>• Limited exemptions in relation to electronic money are not supported by the NRA conclusions. External accountants and VASPs have not been properly designated. Exemption form application of the AMLTFL provisions does not exclude other providers of money remittance activities, the exemption is applied not from some requirements under AMLTFL but form all.<br>• Croatia requires REs to take enhanced measures to manage and mitigate "high", rather than "higher" ML/TF risks. The 2020 NRA recommended that CDD threshold be reduced for authorised exchange offices, but this was not included in the 2020 NRA Action Plan to take action.<br>• When applying Simplified measures there is no clear requirement for REs to ensure that this is done consistent with the ML/TF risks.<br>• Deficiencies under R.26 and 28 have an impact on Croatia's compliance with criterion 1.9.<br>• Simplified CDD is permitted only where "low" rather than "lower" risk has been identified and deficiencies in c1.9 apply. |
| 2. National co–operation and coordination | **PC** | • Croatia does not have a national AML/CFT policy.<br>• Croatia does not have designated authority or coordination mechanism that holds responsibility for the national AML/CFT policies.<br>• The IIWG does not include all authorities responsible for AML/CFT as provided in AMLTFL (Art.120).<br>• Co–operation on PF is not substantiated. |
| 3. Money laundering offences | **LC** | • There is a minor gap in the range of predicate offences related to TF.<br>• Criminalisation of self–laundering is not in line with the requirements. |

| | | |
|---|---|---|
| | | • Sanction applied to natural and legal persons are not proportionate and dissuasive. |
| 4. Confiscation and provisional measures | **LC** | • There is no mandatory confiscation of instrumentalities intended for use in the commission of the majority of predicate offences.<br>• Confiscation of corresponding value for instrumentalities is not provided.<br>• There is no definition of "funds".<br>• There are unreasonable restrictions do exist in relation to the seizure of objects related to the offence and relevant for the investigation.<br>• Management of the seized legal persons is not regulated. |
| 5. Terrorist financing offence | **LC** | • TF offence does not include all of the elements of the offences in the treaties listed in the Annex to the TF Convention.<br>• CC does not contain definition of "funds and other assets" and, therefore, it is not evident that it is in line with the Standards.<br>• Financing of travel for the purpose of preparation of a terrorist act is not considered as a criminal offence.<br>• Range of sanctions applicable for legal persons is not dissuasive. |
| 6. Targeted financial sanctions related to terrorism & TF | **PC** | • There is no competent authority or mechanism identified for proposing persons and entities for designation to 1267/1989 and 1988 UN Committees.<br>• There is no formal procedure in place establishing the process for detection and identification of targets for designation based on the designation criteria set out in the UNSCRs.<br>• There are no specific evidentiary standards defined for deciding whether or not to make a proposal for designation to 1267/1989 and 1988 UN Committees.<br>• There are no procedures in place with respect to filing information with UN Sanctions Regimes in support of proposed designations.<br>• There is no requirement on information to be provided in support of the proposed designation.<br>• No provision exists indicating whether Croatia may be made known to be the designating state.<br>• There is no explicit provision defining the competent authority of a mechanism for making a designation pursuant to UNSCR 1373 at a national level.<br>• There is no mechanism for identifying targets for designation based on the designation criteria set out in UNSCR 1373, at national level.<br>• There is no formal procedure for prompt determination of designation requests received from non–EU Member States pursuant to UNSCR 1373, at national level.<br>• There are no specific evidentiary standards defined for deciding whether or not to make a proposal for designation pursuant to UNSCR 1373, at national level.<br>• There is no formalised procedure under which Croatia could ask another country to give effect to undertaken freezing measures.<br>• No information is provided on an empowered competent authority and procedures and mechanisms to follow for collection of information on persons that meet designation criteria, at national level. |

| | | |
|---|---|---|
| | | • There is no explicit provision for operation *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered, at national level.<br>• TFS are not implemented "without delay".<br>• The requirement to freeze the funds and assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities and the funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities, is not covered under the IRM Law.<br>• The prohibition from making the assets available wholly or jointly, for the benefit of designated persons, entities owned or controlled, directly or indirectly by designated persons, are not covered under the IRM Law.<br>• There is no mechanism for active communication of designations to FIs and DNFBPs.<br>• No guidance is provided to REs on their obligation in taking actions under freezing mechanism.<br>• No requirements are in place on reporting attempted transactions.<br>• there is no specific rule for the protection of *bona fide* third parties acting in good faith when implementing the obligation under UNSCRs.<br>• There is no specific procedure for submitting de–listing requests to the relevant UN Sanctions Committee, at national level.<br>• There is no procedure or mechanism set at national level for de–listing and unfreezing the funds and other asset that no longer meet the designation criteria pursuant to UNSCR 1373.<br>• There is no publicly known procedure for revision of the designation decision taken pursuant to UNSCR 1373, at national level.<br>• There is no publicly known procedure, *at national level,* to facilitate review by the *1988 Committee.*<br>• There is no publicly known procedure, *at national level,* for informing designated persons and entities of the availability of the *United Nations Office of the Ombudsperson*, pursuant to UNSCRs 1904, 1989, and 2083 to accept de–listing petitions.<br>• There is no publicly known procedure, *at national level,* to unfreeze the funds or other assets of persons or entities inadvertently affected by a freezing mechanism.<br>• There is no information or guidance provided on ensuring timely communication of de–listings and unfreezing to FIs and DNFBP sectors, and defining their obligations to respect a de–listing or unfreezing actions. |
| 7. Targeted financial sanctions related to proliferation | **PC** | • TFS are not implemented "without delay".<br>• The requirement to freeze the funds and assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities and the funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities, is not covered under the IRM Law.<br>• There is no mechanism for active communication of designations to FIs and DNFBPs.<br>• No guidance is provided to REs on their obligation in taking actions under freezing mechanism.<br>• No requirements are in place on reporting attempted transactions. |

| | | |
|---|---|---|
| | | • There is no specific rule for the protection of *bona fide* third parties acting in good faith when implementing the obligation under UNSCRs.<br>• There is no power provided to supervisory authorities for monitoring compliance and applying sanction for implementation of UN PF–related TFS.<br>• There is no specific procedure to petition a request for de–listing at the Focal Point or informing the designated person to petition to Focal point.<br>• There is no publicly known procedure, *at national level,* to unfreeze the funds or other assets of persons or entities inadvertently affected by a freezing mechanism.<br>• There is no information or guidance provided on ensuring timely communication of de–listings and unfreezing to FIs and DNFBP sectors and defining their obligations to respect a de–listing or unfreezing actions.<br>• When permitting additions to the accounts, there is no provision specifying the payments due under contracts, agreements or obligations should have been raised prior to the date on which the property became subject to freezing, at a national level.<br>• There is no regulation on authorising making payments under a contract entered into prior to designation. |
| 8. Non–profit organisations | **PC** | • Subset of NPOs that fall under the FATF definition and are likely to be at risk of TF abuse is not identified.<br>• Croatia has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk, as well as how terrorist actors abuse those NPOs.<br>• Croatia has not reviewed the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for terrorism financing support.<br>• Not enough measures are taken to promote public confidence in the administration and management of NPOs.<br>• Outreach conducted by Croatia does not sufficiently cover the risks to which NPOs are exposed in their business activity.<br>• No outreach and educational programmes to raise and deepen awareness among the donor community on the potential vulnerabilities of NPOs to TF abuse and TF risks was provided.<br>• No targeted outreach and educational programmes to raise and deepen awareness among the NPOs on their potential vulnerabilities to TF abuse and TF risks, and on measures that NPOs can take to protect themselves against such abuse was provided.<br>• Croatia did not co–operate with the NPO sector in developing and refining best practices to address TF risks.Cash restriction requirement that also applies to NPOs does not constitute encouragement to use regulated financial channels when conducting transactions below the set threshold.<br>• Croatia did not demonstrate that risk–based supervisory measures apply to NPOs at risk of terrorist financing abuse. Measures foreseen under paragraph 6b(v)of INR.8 are not implemented.<br>• Supervisory measures do not focus specifically on implementation of the R.8 by the NPOs. No specific sanctions are available for non–compliance of NPO with R.8 requirements. |

| | | |
|---|---|---|
| | | • Croatia has not identified specific points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support. |
| 9. Financial institution secrecy laws | **C** | • |
| 10. Customer due diligence | **PC** | • The AMLTFL allows anonymous accounts, passbooks, safe deposit boxes or other anonymous products, that existed as of 2019 to continue until such time as possible to remediate and in any case prior to any use thereof, the effect of which is to freeze the account.<br>• AMLTFL (Art. 16(1) sets not defined conditions for obligation to carry out CDD measures.<br>• Conflicting legal provisions on the CDD requirements for authorised exchange offices.<br>• No requirement for the identification or verification of foreign trusts or similar legal arrangements.<br>• Exceptions to identification and verification requirements are not based on a proven low risk assessment.<br>• No requirement for the collation of reliable information or data to assist in the verification of the identify of a BO.<br>• REs are not required to understand the purpose and intended nature of a business relationship.<br>• There is no requirement for regular reviews to ensure that CDD documents and data is up to date.<br>• There are no provisions which require REs to obtain information on the powers that regulate and bind the legal persons or legal arrangements.<br>• Reference to indirect ownership only considers it through legal arrangements and does not include legal persons.<br>• Trusts or similar legal arrangements whose trustee resides in a foreign jurisdiction are not subject to CDD obligations.<br>• There is no requirement to take into account previously obtained CDD, nor to consider materiality.<br>• There are no provisions which exempt REs from CDD in case of suspicions of ML/TF and instead submit an STR if they reasonably believe that completed CDD could tip off the customer. |
| 11. Record keeping | **LC** | • The requirement to keep records is limited to analysis undertaken in relation to complex and unusual transactions only.<br>• No requirement for FI to keep records to allow transactions to be reconstructed. |
| 12. Politically exposed persons | **LC** | • While a reference to domestic PEPs is not explicitly mentioned, Croatia considers that domestic PEPs are covered because Croatia is an EU–Member State.<br>• There is no obligation on REs to consider making an STR when higher risk of ML/TF is identified in connection with a life insurance policy whose beneficiary or BO is a PEP. |
| 13. Correspondent banking | **PC** | • Requirements for the establishment of correspondent banking relationships is limited to non–EU/EEA. The provisions in respect to EU/EEA correspondent banking relationships are only applicable where increased risks are identified. |

| | | |
|---|---|---|
| 14. Money or value transfer services | **LC** | • There are no legal provisions requiring a competent authority to monitor and identify unlicensed activities<br>• There is no explicit requirement to include monitoring and compliance with AML/CFT programmes as part of the on–site or off–site checks of branches and agents. |
| 15. New technologies | **PC** | • There is no legal obligation for assessment of ML/FT risks associated with new products or services.<br>• There are no licensing or registration requirements for VASPs<br>• Only some VASP activities are subject to AML/CFT supervision and sanctioning. The scope of a VASP in Croatia does not fully comply with the FATF's definition of a VASP.<br>• There is no explicit requirement for the CFSSA, or other authority, to identify natural or legal persons carrying on VASP activities.<br>• Limited guidelines or feedback has been issued to the new VASP sector<br>• The occasional transactions designated threshold above which VASPs are required to conduct CDD is not determined to be USD/EUR 1 000<br>• There are no legal requirements obliging originating and beneficiary VASPs to obtain and hold information in respect to virtual asset transactions<br>• The CFSSA, as competent authority for VASPs, is only able to co–operate and exchange information in relation to the supervision of VASPs with non–EU counterparts |
| 16. Wire transfers | **LC** | • The deficiencies noted within R.6 and R.7 impact R.16. |
| 17. Reliance on third parties | **PC** | • There is no requirement for the FI to satisfy itself that the third party is regulated and supervised or monitored and has measures in place to comply with R. 10 and R.11 requirements.<br>• There is no obligation for FIs to have regard to information on the level of country risk when determining which country, the third party can be based in.<br>• No provisions are set on the level of the ML/TF risk that may have a third party from an EU Member State.<br>• There is a limited requirement set for the CDD, record keeping requirements and programs against ML/TF in line with R. 10 – 12 and 18.<br>• No provision to regulate mitigation of higher country risks by group policies is set. |
| 18. Internal controls and foreign branches and subsidiaries | **PC** | • Appointment of a compliance officer at management level is not dependent on a defined size and nature of business operations<br>• There is a lack or requirement to appoint have an independent audit function, if appropriate, save for banks and FIs under the supervision of the CFSSA.<br>• There are no requirements for financial groups to implement group–wide programs against ML/TF.<br>• There are no specific requirements for exchanges of CDD and customer, account and transaction information for ML/TF risk management purposes within the group.<br>• No specific provision to safeguard information to prevent tipping off. |

| | | |
|---|---|---|
| | | • No requirement to check branches subsidiaries in EU Member States apply AML/CFT measures equivalent to Croatia and if appropriate apply additional ML/TF measures. |
| 19. Higher–risk countries | **LC** | • FIs apply EDD in line with EC requirements and high risk third country list which lacks specific reference to FATF named countries until added to EU list. This affects all requirements under R.19. |
| 20. Reporting of suspicious transaction | **LC** | • STRS can be filed the following day if not possible before carrying out the ST, where undefined "justifiable" reasons are present.<br>• The AMLTFL does not explicitly cover financing of travel for terrorist purposes as required by UNSCR 2178 (2014). |
| 21. Tipping–off and confidentiality | **LC** | • There is no explicit protection for directors from both criminal and civil liability.<br>• There is no explicit prohibition from disclosing STR filed or sanction for such disclosure. |
| 22. DNFBPs: Customer due diligence | **PC** | • The deficiencies noted in R.10, R.11, 12, R.15 and R.17 also apply to DNFBPs and hence impact R.22.<br>• There are no provisions to require Casinos to link CDD information to transactions undertake by the customer<br>• CDD requirements for real estate in respect to both purchasers and vendors are set in guidelines and not as a legal obligation.<br>• There is a legal uncertainty as to whether DPMSs, are required to implement all CDD measures (apart from identifying and verifying the customer).<br>• Auditors and external accountants are not subject to R.22 as are not covered under the listed activities. |
| 23. DNFBPs: Other measures | **PC** | • The deficiencies identified in R18, R.19, R.20 and R.21 also apply in relation to DNFBPs. |
| 24. Transparency and beneficial ownership of legal persons | **PC** | • The NRAs do not comprehensively assess the ML/TF risks and vulnerabilities associated with all types of legal persons that may be set up in Croatia.<br>• Not all Legal persons are not required to maintain the basic information set out under c. 24.4 themselves separately to the relevant register.<br>• There are no obligations for legal persons to keep details of members, retain lists of shareholders or members in Croatia, or notify the relevant register where the information is held.<br>• There is a lack of explicit obligations to update the required basic information in terms of types, amounts and holders of shares and the length of time such registers should be held. There are no mechanisms to test/verify the basic or beneficial ownership information in the Court register, Register of Associations/ foundations or beneficial ownership register or any changes to that information.<br>• It is questionable whether the 15 day time limit for providing the AMLO beneficial information and the 30 day time limit for updating the BO register is "timely" or accurate c10.10 discusses shortcomings of the definition of BO.<br>• There is a gap of 15,000 legal persons in beneficial ownership register and no sanctions for failing to file such information have been imposed. or for those responsible for updating the BO register should be resident in Croatia. |

| | | |
|---|---|---|
| | | • Timeframes are not specified for retention of lists of members for Associations, company accounts and documents (including shareholder information) for LLCs and JCS.<br>• Supervisors have to rely on generic powers to obtain documents under AMLTFL/Sector Specific laws as there is no explicit provisions for REs to provide them with CDD and BO information.<br>• Bearer shares (issued only by JSCs), already in existence pre–2008, are not banned and while there is no explicit requirement they should be registered, no benefit can be obtained from them unless they are registered.<br>• No explicit prohibition of nominee shareholders or nominee directors in Croatia.<br>• The Associations Law and the Foundations Law do not apportion liability or prescribe sanctions for violations although supervisory action can be taken, and fines may be imposed (Art. 139 General Administrative Procedure Act)<br>• There are deficiencies identified in R. 37–40 are relevant to international co–operation on rapid provision of basic information.<br>• The AMLO and Police don't monitor and keep ratings on the quality and usefulness of basic and beneficial ownership information received from foreign FIUs. |
| 25. Transparency and beneficial ownership of legal arrangements | **LC** | • External accountants are not considered REs regarding trusts and are not obliged to hold information on trusts they establish, operate or manage.<br>• Deficiencies in 10.9 and 10.11 relating to obligations identify and verify foreign trusts, legal arrangements, and their beneficial owners.<br>• No checks or verification of changes to information in BO register are conducted generally.<br>• There is a lack of explicit legal powers for authorities to obtain information on trusts or other legal arrangements and limitation on Accountants as REs re Trusts<br>• It is questionable how the availability of BO information of foreign trusts is being ensured and whether the 15 day time limit for providing the AMLO beneficial information is "timely"<br>• Deficiencies identified in R. 37–40 are relevant in relation to the exchange of information on foreign trusts/legal arrangements that may be obtained through Croatia REs<br>• The range of sanctions for trustees who do not adhere to obligation to hold accurate BO information and update the BO registry are not considered dissuasive. |
| 26. Regulation and supervision of financial institutions | **LC** | • Croatia has not been subject to an assessment against all the relevant principles (primarily IOSCO and IAIS)<br>• Provisions for group supervision is limited to financial groups part of a foreign FI.<br>• There are no legal provisions establishing the periodic assessment of a group. |
| 27. Powers of supervisors | **LC** | •<br>• The deficiencies identified in R.35 apply |
| 28. Regulation and supervision of DNFBPs | **LC** | • In respect to Games of Chance, there is no provision requiring the supervisory authority to consider the criminal records of a BO, or key function holder. There is no requirement preventing criminal |

| | | |
|---|---|---|
| | | associates from holding a key function or being the BO of a Games of Chance. There is no provision ensuring that information on criminal records or the association with criminals would be ensured at any time after licensing<br>• There are no licensing obligations for accountants, DPMS and TCSPs. Therefore, there are no provision to prevent criminals or its associates from holding key functions or being the BO of these entities.<br>• Deficiencies noted within R.35 apply. |
| 29. Financial intelligence units | **C** | • This recommendation is fully met. |
| 30. Responsibilities of law enforcement and investigative authorities | **C** | • This recommendation is fully met. |
| 31. Powers of law enforcement and investigative authorities | **LC** | • Temporary seizure is not applicable to files and other documents of state authorities, the publication of which would violate the confidentiality obligation, until decided otherwise by the competent authority. |
| 32. Cash couriers | **PC** | • Regulatory measures apply only to movements (both inward and outward) of cash from and to the EU, these do not extend to physical transportation of cash through container cargo or the shipment of cash through mail. |
| 33. Statistics | **PC** | • Croatian authorities do not maintain adequate statistics on ML/TF investigations, prosecution, and conviction, as well as data on seizure and confiscation.<br>• There is no legislative requirement for maintaining statistics on international co–operation carried out by Police, CA, TA, and supervisory authorities. |
| 34. Guidance and feedback | **C** | • This recommendation is fully met. |
| 35. Sanctions | **PC** | • There are limited sanctions in respect to NPOs, and not fully compliant with the FATF Recommendations.<br>• Reference to "severe" misdemeanours is not defined and therefore it is unclear what this comprises.<br>• Definition of "Senior management of the RE" clarifies that "it does not have to be, in all cases, a member of the management board or another managerial body".<br>• The sanctions available cannot be considered as dissuasive. |
| 36. International instruments | **PC** | • Croatia did not ratify the 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.<br>• Croatia did not ratify the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.<br>• Some deficiencies are identified with regard to the implementation of the provisions of the Palermo Convention, Merida Convention and the TF Convention (see also R.5). |
| 37. Mutual legal assistance | **LC** | • There is no regulation on the prioritisation or timeframes for execution of international requests, in particular with non–EU Member States.<br>• The treatment of requests from non–EU Member States concerning fiscal offences is contradictory.<br>• The confidentiality obligation is limited. |

| | | |
|---|---|---|
| | | • The specified list of offences which do not require dual criminality for conductive coercive actions is not exhaustive.<br>• There are no legal provisions regarding the use of investigative techniques in the framework of direct co–operation between foreign judicial or LEAs and domestic counterparts. |
| 38. Mutual legal assistance: freezing and confiscation | **PC** | • The legislator does not specify whether the instrumentalities would also include the ones that are intended for use. The powers to confiscate these objects are not specified either.<br>• There are no explicit provisions regarding non–conviction–based provisions.<br>• Croatia does not have arrangements in place for coordinating seizure and confiscation actions with foreign countries on the basis of bilateral and multilateral agreements.<br>• No information has been provided on the sharing of assets with non–EU countries. |
| 39. Extradition | **LC** | Deficiencies identified under R.3 and R.5, apply. |
| 40. Other forms of international co–operation | **PC** | • The CNB, the Financial Inspectorate and the TA do not seem to have clear and secure channels to exchange information with their foreign counterparts.<br>• The TA, Financial Inspectorate and CA do not have formal mechanisms for prioritisation of international requests.<br>• Some MoUs signed by the CFSSA contain unduly restrictions on the exchange of information with foreign counterparts.<br>• The FI and TA do not have safeguards in place to ensure that the information exchanged is used solely for the purpose it was provided.<br>• There are no legal provisions for the CNB, FI, CFSSA and TA to ensure an adequate level of protection to the information provided to non–EU countries. EU countries are not covered at all.<br>• Legal provisions do not specify the type of information that supervisors can exchange.<br>• There are no legal provisions allowing foreign supervisors to conduct inquiries themselves in Croatia.<br>• Neither the CNB nor the CFSSA provisions envisage cases where the requesting financial supervisor is under a legal obligation to disclose or report the obligation.<br>• No specific legal framework for co–operation is provided for the FI, except the one prescribed under the AMLTFL.<br>• The Police, TA and CA are not obliged to collect and store the requested data for the purposes of their submission to foreign authorities by applying the powers established by national regulations.<br>• There is no information available for co–operation with non–counterparts' competent authorities of non–EU Member States. |

# GLOSSARY OF ACRONYMS[233]

| | DEFINITION |
|---|---|
| AMLTFL | Anti–Money Laundering and Terrorist Financing Law |
| AMLO | Anti–Money Laundering Office |
| BNI | Bearer Negotiable Instruments |
| CC | Criminal Code |
| CDD | Customer Due Diligence |
| CA | Customs Administration |
| CFSSA | Croatian Financial Services Supervisory Agency |
| CFSSA Law | Croatian Financial Services Supervisory Agency Law |
| CNB | Croatian National Bank |
| CTD | Counter Terrorism Department of PNUSKOK |
| DNFBP | Designated Non–Financial Businesses and Professions |
| DPMS | Dealer in Precious Metal Stones |
| EBA | European Banking Authority |
| ECB | European Central Bank |
| EDD | Enhanced Due Diligence |
| ESA | European Supervisory Authorities |
| EU | European Union |
| EUR | Euro |
| FI | Financial Institution |
| FIU | Financial Intelligence Unit |
| FOA NPOs Law | Financial Operations and Accounting of Non–Profit Organisations Law |
| FEL | Foreign Exchange Law |
| GDP | Gross Domestic Product |
| IIWG | Inter–Interinstitutional Working Group for the Prevention of ML/TF |
| IRM Law | International Restrictive Measures Law |
| JCCMEUL | Judicial Co–operation in Criminal Matters with the EU Member States Law |
| LEAs | Law Enforcement Authorities |
| ML | Money laundering |
| MoF | Ministry of Finance |
| MFEA | Ministry of Foreign and European Affairs |
| MoJA | Ministry of Justice and Administration |
| MoI | Ministry of Interior |
| MoU | Memorandum of Understanding |
| MPPCSA | Ministry of Physical Planning, Construction and State Assets |
| MVTS | Money or Value Transfer Services |
| MLA Law | Mutual Legal Assistance in Criminal Matters Law |
| NPO | Non–Profit Organisation |
| NRA | National Risk Assessment |
| OCG | Organised Criminal Group |
| PDPL | Police Duties and Powers Law |
| PEP | Politically Exposed Persons |
| PNUSKOK | Police National Office for Suppression of Corruption and Organised Crime |
| PSL | Payment System Law |
| RBA | Risk–Based Approach |
| RE | Reporting Entity |
| RLP Law | Responsibility of Legal Persons Law |
| SAO | State Attorney's Office |
| SIA | Security and Intelligence Agency |
| SRBs | Self–Regulatory Bodies |
| Standing Group | Standing Group for the Introduction and Monitoring of the Implementation of International Restrictive Measures |
| STR | Suspicious Transaction Report |
| TA | Tax Administration |
| TCSP | Trust and Company Services Providers |

[233] Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

| | |
|---|---|
| TF | Terrorist Financing |
| TFS | Targeted Financial Sanctions |
| Third State | Non – EU Member State |
| UN | United Nations |
| UNSCR | United Nations Security Council |
| USKOK | Office for the Suppression of Corruption and Organised Crime |
| USKOK Law | Office for the Suppression of Corruption and Organised Crime Law |
| WB | World Bank |
| WMD | Weapons of Mass Destruction |

www.coe.int/MONEYVAL

December 2021

Anti-money laundering and counter-terrorism financing measures

# Croatia

*Fifth Round Mutual Evaluation Report*

This report provides a summary of AML/CFT measures in place in Croatia as at the date of the on-site visit (10 - 21 May 2021). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Croatia's AML/CFT system