iPROCEEDS

Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey

Version 16 August 2017

Assessment Report

Findings and Recommendations for improvement of guidelines and indicators for financial sector entities to prevent and detect online fraud and money laundering in the online environment

Montenegro

Project: iPROCEEDS

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1 Introduction

According to the MONEYVAL 2012 Research Report titled "Criminal Money Flows on the Internet", unlike traditional money laundering schemes involving the use of the banking system, cyber-laundering involves sophisticated schemes and relies on various types of operations and financial services providers, ranging from bank transfers, cash withdrawals/deposits, the using of digital/electronic currencies to money mules and money remitting services.[1] Often the chain is "broken" by cash operations performed traditionally by money mules followed sometimes by the use of a traditional payment service. If the respective payment service is integrated with an Internet payment service provider, then the money could immediately be exchanged into digital currency and transferred almost anonymously to another country.

Successful prevention, detection and investigation of cybercrime, proceeds from online crime and online money laundering requires the inclusion of a wide range of stakeholders, and in particular it requires the involvement of financial institutions and other obliged entities under the anti-money and countering financing of terrorism (AML/CFT) legislation, financial intelligence units (FIUs), AML/CFT regulatory and supervisory bodies, cybercrime units, financial investigation units, and prosecution services. Though this criminality can be significantly reduced by raising awareness among the potential victims, its prevention and detection also heavily depends on the readiness of obliged entities to mitigate the risks associated with these offences and their ability to recognise the suspicious patterns related to their clients, products, services and transactions.

In this regard, international AML/CFT standards[2] require that competent authorities and supervisors establish guidelines, which will assist obliged entities in detecting and reporting suspicious transactions related to funds that are proceeds of a criminal activity, or are related to terrorist financing.

This report was prepared by Council of Europe experts, Mick Jameison (The United Kingdom) and Klaudijo Stroligo (Slovenia) under Expected Result 4, activities 4.2.1 and 4.2.2 of the Joint Project of the European Union and the Council of Europe on targeting crime proceeds on the Internet in South Eastern Europe and Turkey – iPROCEEDS.

1.1 Objectives

The main objective of the report is to put forward a set of recommendations for elaboration and/or improvement of guidelines and indicators for financial sector entities to prevent and detect online fraud and money laundering in the online environment. The report is also aiming to address some legal and policy issues

[1] See MONEYVAL 2012 Research Report on criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction, pp. 6 and 38: https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a

[2] See FATF Recommendation 34.

identified during the project cycle that could hamper the effective use of these guidelines and indicators in practice.

1.2 Methodology

In preparing this report, the Council of Europe experts have conducted desk review of the relevant AML/CFT legislation and other documents related to this topic and made use of data and information gathered during the on-site assessment mission to Podgorica, Montenegro on 13-14 June 2017, where they met with representatives of all relevant institutions.[3]

1.2.1 Meetings

Meetings were held with relevant institutions within Montenegro and took the same general format whereby the experts posed questions to the delegation and collected the responses. The topics covered in the meetings were:

- The interpretation of the reporting obligations under the current AML legislation.
- The current general and sector-specific indicators, how they are implemented and supported in practice (e.g. by software or a manual process).
- Whether the current indicators can be used as indicators of online crime proceeds and if not, what other indicators may be required.
- The understanding of the current cybercrime threats and issues relating to online crime proceeds.
- Any statistics available or other concrete measures of number of reports made.
- Any other observations or useful information that the delegation may wish to provide.

The delegates represented the following agencies[4]:

- Administration for Prevention of Money Laundering and Terrorist Financing – Administration (Montenegro Financial Intelligence Unit - FIU);
- Central Bank of Montenegro;
- Commission for Securities;
- Agency for Supervision of Insurance;
- Banks and Banking Association;
- Chamber of Commerce; and
- Money Remittance Providers.

A summary of relevant points identified during the meetings include the following:

- The FIU indicated that it is competent to enforce current and new legislation relating to money laundering and terrorist financing through its mandate and operational activity.

[3] The link to the outline of the meetings is provided in Appendix A.
[4] The Police Cybercrime Unit was unable to attend the meeting and provided written submissions.

- There is a general increase in the use of technology and the Internet within Montenegro, but it is currently less used than in comparable countries in Europe and the Balkans region.
- Customers who use financial services and banking facilities in Montenegro undertake these in a face-to-face system. Those services routinely offered to customers in other countries, such as Internet banking and on-line interactions are not widely implemented. The use of mobile phones and tablets are also restricted in their access to banking and financial services. It was identified that none of the banks in Montenegro offer a banking application that could be used with such devices.
- Customer due diligence (CDD) rules and know your customer (KYC) checks are widely enforced because Montenegro banks and other financial institutions uses the smaller size of its population to increase its familiarity to its customers. The general non-reliance on technology requires customers to personally attend banking and other financial institutions premises to undertake their transactions.
- The threats from crime, money laundering and terrorist financing that are enabled by the Internet (and technology) are reportedly significantly lower than most other countries in Europe and the Balkans region. An important reason is that the Central Bank of Montenegro considers e-banking and similar new products and services as high-risk despite the fact that during the recent national money laundering and terrorist financing risk assessment the e-banking was assessed as low-medium risk for money laundering.
- Cybercrime is generally unreported in Montenegro, albeit Police have investigated reports of malware, ransomware attacks (where business have made payments in bitcoins), CEO fraud and insertion of keylogging devices into victims' computers.
- Cybercrime does occur against banking systems and includes mainly phishing type attacks. Other attacks such as ransomware, hacking and distributed denial of service attacks have occurred, but the impact of such offences was negligible or not detected.
- The Cybercrime Unit (Police) consists of one officer and this potentially limits capacity, capability and an intelligence picture in relation to current threats and typology of cybercrime and related money laundering in Montenegro.
- Intelligence collection, assessment and dissemination takes place in the financial sectors but appears limited to traditional areas of fraud and money laundering.
- The representatives of participating institutions reported that there is a significant knowledge gap in the understanding of many areas and typologies of cybercrime and online money laundering.
- In Montenegro, the remittances are mostly used to receive money from a diaspora (e.g., Germany and USA) and to send money by tourists and temporary workers to their homes (e.g., to Serbia, Bosnia and Herzegovina, Croatia and "the former Yugoslav Republic of Macedonia"). The remittance system in Montenegro only allows to conduct cash transactions and the clients cannot use the credit cards. From June 2015, the Western Union reported 715 suspicious transactions to the FIU.
- Virtual currencies are not regulated in Montenegro. While some virtual payment systems are used within Montenegro, there is reluctance in the banking system to identify opportunities to persons who wish to utilise these

services. The default position in dealing with these systems is to treat customers and transactions as high-risk or prevent interaction with them.

- One suspicious transaction relating to a cybercrime has been reported to the FIU by a local bank. This report was made in 2012 and there have been no other reports directly attributable to cybercrime since.
- In 2016, foreign FIUs sent three requests for assistance to the local FIU, which demonstrated a clear link to cybercrime, but it was found out that they were not related to Montenegro. There are no reports of similar requests in 2017.

1.2.2 Research

A desk review of all relevant legislation has been conducted with the following objectives:

- To find out if the current anti-money laundering and countering financing of terrorism (AML/CFT) legal framework related to detection and reporting of suspicious transactions meets the international AML/CFT standards.
- To assess if the AML/CFT legal framework provides a sufficient legal basis for updating the existing indicators for suspicious transactions to cover also the prevention/detection of online fraud and online money laundering.
- To evaluate the current list of indicators for suspicious transactions in order to identify if some of the indicators can be used also for prevention/detection of online fraud and online money laundering.

To this end, the provisions of the Law on Prevention of Money Laundering and Terrorist Financing (AML/CFT Law)[5], the Criminal Code[6], and the Rulebook on Indicators for recognising suspicious customers and transactions (hereinafter referred to as Rulebook) have been analysed and reviewed. In the assessment provided below, the most recent Council of Europe MONEYVAL Committee mutual evaluation report (MER)[7] on Montenegro and other documents related to criminalisation of online fraud and other criminal offences mentioned in the Council of Europe Budapest Convention on Cybercrime have also been taken into account.[8]

2 Legislation

The Criminal Code prescribes all criminal acts, including computer-related fraud[9] and other offences related to cybercrime[10], generally in line with the Budapest Convention on Cybercrime.[11] The money laundering offence is set out under Article 268 of the Criminal Code and, as regards the predicate offences; it is based on "*all crime*"

[5] See Appendix C.
[6] See Appendix D.
[7] See Appendix E.
[8] See Appendix B.
[9] The computer fraud is criminalised in Article 352 of the Criminal Code.
[10] Articles 349-356 of the Criminal Code deal with specific cybercrime offences. There are other offences within this statute, such as fraud and copyright offences, where the criminal use of computers and computer programs are legislated for.
[11] See the Council of Europe Cybercrime legislation – Country profile - Montenegro.

approach[12]. According to the MONEYVAL 2015 MER on Montenegro, the criminal offence of money laundering is only partially criminalised in compliance with the relevant AML/CFT international standards.[13]

The reporting of suspicious transactions is regulated in Paragraph 2 of Article 41 of the AML/CFT Law, which reads as follows:

"(2) *A reporting entity shall, without delay, provide to the Administration the data from Article 79 of this Law in all cases when in relation to the transaction (regardless of the amount and type) or customer there is a suspicion of money laundering or terrorist financing."*

In Paragraphs 7 and 8 of the same article it is also stated:

"(7) Provisions from paragraphs 2, 3 and 4 of this Article shall apply to an announced transaction as well.
(8) The manner and conditions of providing the data from paragraphs 1 - 7 of this Article shall be more specifically defined by the Ministry."

In this regard, it is important to mention also a definition of "*suspicious transaction*" as provided in Article 5, point 11 of the AML/CFT Law:

"Suspicious transaction means any transaction for which it is deemed, based on indicators for recognising suspicious transactions and customers defined by this Law, bylaws, and internal procedures of reporting entity, that the transaction or a person conducting it are related to a suspicion of money laundering and terrorist financing."

The analysis of these provisions shows that it is not fully compliant with the Financial Action Task Force (FATF) Recommendation 20[14] and Article 33 of the EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[15], which require reporting to the FIU any suspicion that the funds are the proceeds of criminal activity, or are related to terrorist financing. As it can be seen from the text above, Paragraph 2 of Article 41 and the definition of suspicious transaction in Article 5 only cover transactions related to money laundering and terrorist financing and not also transactions with funds that are the proceeds of other criminal offences[16]. This deficiency was identified also by MONEYVAL in its MER on Montenegro.[17]

[12] This means that all criminal offences, including cybercrime related offences, are predicate offences for money laundering. See the MONEYVAL 2015 Report on Fourth Assessment Visit to Montenegro, page 38.
[13] Ibidem; pages 35-47.
[14] See the FATF 2012 Forty Recommendations (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html).
[15] See the Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= celex%3A32015L0849).
[16] The draft new AML/CFT Law, which at the moment of the on-site visit was pending approval of the Government, is addressing this issue in line with the international AML/CFT standards.
[17] See the MONEYVAL 2015 Report on Fourth Assessment Visit to Montenegro, pages 153-162.

The AML/CFT Law in Articles 53 and 54 further requires that when establishing a suspicion of money laundering or terrorist financing and other circumstances related to the suspicion, all obliged entities shall use the list of indicators for identifying suspicious customers and transactions. This list should be defined by the Ministry of Finance based on a proposal prepared by the FIU in cooperation with other competent bodies. In the same context, Article 56 of the AML/CFT Law stipulates that the FIU should prepare and compile the list of indicators and submit it to the reporting entities. Based on these provisions, in November 2014 the Ministry of Finance adopted the Rulebook, which in Annex presents 10 lists of indicators for recognizing suspicious customers and transactions. The Annex includes the general indicators and obliged entities' specific indicators as well as a separate list of indicators for terrorist financing.

It is clear from the above that the current legislative framework fails to require the obliged entities to report to the FIU any suspicion of criminal activity or attempted criminal activity, including the online fraud, beyond money laundering and terrorist financing.

As regards the FIU powers, the AML/CFT Law regulates differently situations where the FIU suspects that money laundering or financing of terrorism has taken place from situations where it suspects that (only) other criminal offences have been committed.

For example, the following provisions of the AML/CFT Law apply only when FIU suspects that money laundering or financing of terrorism was committed or attempted:

- Article 58, which regulates the FIU power to request data and documents from the obliged entities;
- Article 60, which regulates the FIU power to request data and documents from the state authorities and public power holders;
- Article 61, which stipulates the FIU power to order a temporary suspension of transaction;
- Article 63, which regulates the FIU power to request an on-going monitoring of customer's financial businesses;
- Article 65, which regulates the FIU obligation to submit its report and related documents to the competent authorities; and
- Article 67, which requires FIU to provide feedback to obliged entities on all reported STRs.

On the other hand, the AML/CFT Law in Article 66 authorises the FIU to submit written information to the competent authorities when it evaluates that in relation to a transaction or person there is a suspicion of committing other criminal acts that are prosecuted ex officio.

In practice, this means that if, for example, a suspicious transaction related to an attempted online fraud is reported by the bank to FIU, the latter is formally not allowed to suspend it or to order the monitoring of the victim's or/and suspect's accounts; however, it may send this information and its analysis to the competent law enforcement authority/prosecutor.

3 Typologies and Selected Case Studies

In 2016 the FIU received three requests from foreign FIUs related to cybercrime, but none of these cases led to any investigation since there were no links with Montenegro.

The brief details of these cases are summarised here:

- A request was received from a foreign FIU related to persons who hacked the system of a bank and issued unauthorized payment instructions transferring funds to four accounts.
- Another request was related to persons who attacked the computer system of the Central Bank of the requesting country, and made 35 payment instructions to send money to a bank in another country. Of these transactions, 5 orders were executed and the bank blocked the remaining 30.
- The third request was received from a foreign FIU related to persons suspected of committing Internet fraud in the requesting country's bank. It appeared that unknown persons had opened 36 debit cards with a bank in the requesting country. Later on, via a malicious software, cards were credited with a huge amount of money, which was withdrawn in cash in 15 diferrent countries.

The FIU reported that its only suspicious transaction report (STR) that related to cybercrime in Montenegro was submitted by a local bank in 2012:

- This case related to a Serbian criminal, who had allegedly defrauded a natural person in the UK, and who with assistance of Montenegro criminals transferred €170,000 from the UK to a bank in Montenegro.
- The Montenegrin citizens, who were acting as mules (unemployed), withdrew money from the banks in cash.
- As a result of the STR, the FIU postponed the second transaction and reported the case to Police and Prosecutor's Office.
- This intervention led to the second amount of money being returned to the UK.

The Cybercrime Unit has investigated the following types of cases:

Typology 1: Executed malware allowing attackers remote access to computer devices.

Typology 2: Physical insertion of devices such as key-loggers

- These have been deployed against private companies' computer systems.
- This illegal access has allowed attackers to obtain confidential information such as email and social network credentials or data that was used to defraud companies.
- The scale of these attacks has remained small. Larger attacks against computer servers, which may have allowed the compromise of larger quantities of data, have not been reported to the Cybercrime Unit.

Typology 3: CEO fraud

- Criminals had compromised email accounts and sent messages from such accounts to staff of some businesses in Montenegro directing that payments be made into accounts under their control.
- A staff member has been duped into following the directions in the false email request.
- Money has been transferred to international jurisdictions, such as Italy, UK, Poland, China and Hong Kong.

Typology 4: Ransomware attacks

- Criminals using malware encrypt to computers (ransomware).
- The victims receive a demand of a payment, which will result in the decryption of the data.
- A small number of companies have paid an extortion demand using bitcoins.

The Central Bank of Montenegro reported one significant case that occurred in 2015 when a CEO type attack occurred against a bank. An email was received from a VIP client to arrange a transfer of €1.5 million to an overseas account, which was authorised. However, after the indicators were alerted and action undertaken the money was successfully returned to the victims account.

Western Union reported that they detected frauds related to persons conducting advance payments for (non-existing) cars.

4 Indicators

As mentioned above, the indicators for suspicious customers and transactions are provided in Annex to the Rulebook issued by the Ministry of Finance.

During the on-site expert mission, it was found out that the Central Bank through its management of the Montenegro banking sector is able to ensure that banks adhere to the money laundering and terrorist financing rules that are prescribed by the Ministry of Finance. One of the ways it does this is to require that in addition to the indicators issued by the Ministry of Finance all banks must have also their own indicators for recognizing suspicious transactions that are specific for their businesses.

Moreover, all banks are required to employ a competent IT security person who is directly responsible for assessment of computer systems in banks within Montenegro. The Central Bank indicated that they were satisfied that cybersecurity methodology was embedded into banking sector to a sufficient level. When a cybercrime is committed against a bank, there is a requirement for them to report the matter to the Central Bank only if the damage exceeds 1% of the banks' own funds.

The Commission for Securities reported that the obliged entities in the capital market did not develop any additional indicators for recognising suspicious customers and transactions. Except for the brokerage houses that operate within the banks, all other players in this sector do not use any specific software for detecting suspicious transactions and they rely on Excel templates.

The Agency for Supervision of Insurance identified that they are implementing their own additional measures to control risks. They indicated that they are seeking to improve their standards of flags, money laundering management processes and financial reporting with the industry and legislation, whilst seeking to ensure that some uniform standards are adopted and controls and flags are more harmonised. It appears that many persons working in the insurance sector are unaware of controls and red flags.

The delegates from the Money Remittance Providers (Western Union and Post Office) reported that they undertake a variety of activities to stop their customers sending money to scams and fake adverts. According to Western Union there is a clear awareness about such frauds, which are often conducted online amongst these providers. As regards the indicators for recognizing suspicious transactions the Western Union has developed additional indicators, whereas the Post Office has not.

The analysis of the indicators issued by the Ministry of Finance shows that there are no cybercrime specific indicators included in the lists of indicators and that these indicators do not cover online fraud and online money laundering scenarios that have been identified during the on-site expert mission.

Nevertheless, some of the existing general indicators and indicators related to the banking sector have been identified that can also assist obliged entities in preventing/detecting online frauds[18] and online money laundering. These indicators can be divided into those that apply to the victim's account and those that are relevant for the suspect's/fraudster's account or to both.

a) Indicators applying to the victim's account:

- The amount of electronically transferred funds is inconsistent with the usual business transactions of that customer (Rulebook, List of indicators for banks – Electronic funds transfers, Point 3).

b) Indicators applying to the suspect's account:

- Customer's business transactions are not in accordance with customer's known income or property (Rulebook, General indicators, Point 2).
- There are data that customer is allegedly involved in for illegal activities (Rulebook, General indicators, Point 5).
- Transaction that customer executes is not in accordance with his usual business practice (Rulebook, General indicators, Point 8).
- Transfers of small amounts involving the same persons via other alternative money transfer systems are frequent (Rulebook, General indicators, Point 24).
- Significant fund transfers onto the accounts where no transactions have been executed (inactive accounts), followed by immediate withdrawal of funds, i.e. cash withdrawal (Rulebook, General indicators, Point 27).
- Information from reliable sources (including media or other open sources), indicating that the customer is involved in some illegal activities (Rulebook, General indicators, Point 28).

[18] CEO/BEC frauds in particular.

- New or prospective customer is known as a person involved in illegal activities or is known for criminal activities (Rulebook, General indicators, Point 29).
- Customer conducts cash transactions, which are slightly below the reporting threshold in order to avoid the reporting requirement (Rulebook, List of indicators for banks – Cash Transactions, Point 8).
- Opening accounts of legal entities where deposits inconsistent with the scope of business of the customer are made (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 3).
- Transactions that are not economically justified (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 4).
- Multiple transactions carried out by several different persons to one account and without clear purpose (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 10).
- Attempt to open an account under a false name (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 12).
- Transactions including withdrawal of funds soon after the funds have been deposited at reporting entity (only pass through the account), when this rapid withdrawal of funds is not justified in the business activity of a customer (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 23).
- Depositing or withdrawing higher amounts of effective money (in Euro currency or some other foreign currency) which significantly vary from the customer's usual transactions because they are not in accordance with incomes or customer's status, particularly if the transactions are not typical for the business activities of a customer (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 32).
- Frequent remittances, domestic and foreign, in lower amounts and on going – the so-called linked transactions, with the purpose of concealing the actual amount of funds in the transaction (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 39).
- Founders of the company are identified as suspicious by law enforcement or other sources (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 9).
- There are valid reasons to believe that the documents submitted when opening an account are forged or their authenticity cannot be verified (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 10).
- Customer has never been employed, but owns considerable amounts of funds on the accounts (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 19).
- Customer transfers funds on the account within the country, but their business entity until then has not had any business relationships with that account or receives remittances from business entities with which he has had no connections or previous transfers (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 25).
- Customer frequently deposits or withdraws funds in the amounts that are just below the threshold required for identifying and reporting (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 30).
- Customer executes transactions in high amounts and through an account that has been inactive for a long period of time and possibly gives order for closing

an account (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 33).

- Natural person orders to a bank to transfer funds to a third person without evidence on the purpose and intention of this transfer (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 37).

c) Indicators applying to both victim's and suspect's accounts:

- Customer provides inadequate explanation why does he, in the last moment, change names of persons that are used in relation with the transaction (Rulebook, General indicators, Point 11).
- Customer conducts transactions, which are unusual for him (Rulebook, List of indicators for banks – Cash Transactions, Point 9).
- Transactions related to payment operations in the country and abroad which are inconsistent with the usual business activity of the customer with regard to the goods, amounts, business partners, scope of turnover, etc. (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 5).
- Short term inflows of a large sum of money on a customer's account that has been inactive for a long time or payment on account in an offshore region (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 9).
- Transactions involving several accounts, some of which have been inactive for a long period of time (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 14).
- Transactions with a country that is considered as non-cooperative one by Financial Action Task Force (FATF), or business relationships with customers whose permanent residence is in such countries (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 28).
- Transactions, which are by bank's employees, upon their experience and knowledge, designated as suspicious (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 37).
- There is no evidence on transactions (data on sender), or provided evidence for a transaction does not correspond to the swift message and other data for payment (contract, invoice, preliminary calculation, annexes to a contract etc.) (Rulebook, List of indicators for banks – Unusual changes on the accounts, Point 40).
- Customer insists that a transaction is conducted promptly (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 11).
- Customer or the beneficiary of the remittance is the citizen of the country that does not apply AML regulations, or which is on the consolidated list of the Sanctions Committee on the basis of UN Security Council Resolution 1267 (Rulebook, List of indicators for banks – Behaviour of customers and employees, Point 26).
- Customer executes transactions involving countries known for high level of bank and business secrecy, except in case of those countries that have accepted international AML standards (Rulebook, List of indicators for banks – Electronic funds transfers, Point 5).
- Customer executes electronic fund transfer in/from free or off shore zone, even though such activity is not usual for customer's business activities (Rulebook, List of indicators for banks – Electronic funds transfers, Point 6).

5 Recommendations

Based on the findings during the on-site meetings with the authorities and the desk review of the AML/CFT legislation and other relevant documents, a number of issues have been highlighted in respect of which the obliged entities, the FIU and/or other competent authorities may wish to consider possible improvements in the way in which the online fraud and money laundering are prevented, detected and reported. This report contains a set of recommendations intended to improve the current AML/CFT legislative framework and the existing list of indicators for suspicious transactions related to these topics.

5.1 Legal/Policy Recommendations

This section provides legal and policy recommendations related to selected legal aspects of the obliged entities' reporting obligations and related FIU powers.

- The obliged entities' obligation to report suspicious transaction (Article 41, Paragraph 2 of the AML/CFT Law) and the definition of "suspicious transaction" (Article 5, point 11 of the AML/CFT Law) should be extended so that in addition to suspicion of money laundering and terrorist financing both provisions include also a suspicion of other criminal offences (e.g., suspicion that funds are the proceeds of any criminal activity).
- Along the same line, a reference to the "list of indicators for identifying suspicious customers and transactions" in Articles 53, 54 and 56 of the AML/CFT Law should be extended to ensure that the list of indicators cover (also) a suspicion that funds are the proceeds of any criminal activity.
- The authorities should consider extending the FIU powers: i) to request data and documents from the obliged entities (Article 58 of the AML/CFT Law), ii) to request data and documents from the state authorities and public power holders (Article 60 of the AML/CFT Law), iii) to order a temporary suspension of transaction (Article 61 of the AML/CFT Law), iv) to request an on-going monitoring of customer's financial businesses (Article 63 of the AML/CFT Law), and v) the FIU obligation to provide feedback to obliged entities on all reported STRs (Article 67 of the AML/CFT Law), to cover also situations, when the FIU suspects that an online fraud or another criminal offence has been committed, or attempted, with no suspicion of money laundering or terrorist financing whatsoever.
- FIU, competent law enforcement and prosecutorial authorities should keep unified statistics on detected/reported/investigated online frauds (such as CEO/BEC) across reporting entities.
- The authorities may wish to consider taking part in/drafting a regional blacklist for fraudulently used IBAN accounts, that are known, or suspected, to belong to fraudsters.

5.2 Indicators

This section presents examples of additional indicators for prevention and detection of online fraud and money laundering that the FIU and/or other competent authorities may wish to consider including in the list of indicators for suspicious transactions. In

this regard, the authorities may use the existing structure of the guidelines for indicators for suspicious transactions in the Rulebook (e.g., division per entity/product/transaction) or include an additional section with indicators that will only target the online fraud, other cybercrime offences and related money laundering.

General indicators:

- The transaction is related to the buying or selling the virtual currency (e.g., Bitcoins, Litecoin, Ethereum, Zcash).
- The transaction is related to transfer of winnings from an online gambling platform.
- The client requests a transaction to be carried out urgently or that it should be treated as confidential.

Indicators related to bank accounts/transactions:

- The client receives a payment via Internet based payment services (e.g., PayPal, Payoneer card) that does not include details of the sender or purpose of the transaction.
- The client sends a request for payment late on Friday afternoon for transfers to customers in countries in a time zone where there are still several hours of banking available.
- The client makes withdrawals of funds received from a foreign jurisdiction where the transfer was made near to the close of business in the foreign jurisdiction and the withdrawals are made after close of business, particularly after close of business on Friday, in the foreign jurisdiction.
- Significant language errors or unusual content are identified in e-mail or fax communication between the bank and its client or in the documents presented to the bank by its client.
- The client is ordering a payment to be made to a beneficiary only communicates with the beneficiary via e-mail.
- The total turnover of the account changes suddenly and significantly as compared to the account's long-term average.
- Funds for goods/services are refunded onto a credit card other than the one used to make the original purchase.
- A credit card is issued in an offshore jurisdiction or in a high-risk country and used to withdraw funds from the ATM in Montenegro.

Indicators related to legal persons and business transactions:

- The corporate client with an established relationship changes the payee account details (e.g., IBAN code) for a known beneficiary.
- The corporate client with an established relationship requests a payment to be made to a suspicious "first time" beneficiary.
- There is a mismatch between the name of the payee in the payment instructions and in the account details (e.g., IBAN code).
- The corporate client with an established relationship requests a payment to be made to a payee that has an almost similar name to an existing, known beneficiary.
- Instructions for payment are received from (or on behalf of) a new employee of the corporate client.

Indicators related to geographical risk:

- The transaction involves a country that is known to be associated with online fraud or similar cyber-related criminal activity (on the victim's, suspect's or money mule's side).
- The country of the beneficiary and of the account differs.

Indicators related to remittance services:

- Use of remittance services for the (pre)payment of goods and services ordered online.

6 Appendixes

A. Agenda of the assessment mission of guidelines to prevent and detect/identify online crime proceeds, 13-14 June 2017, Podgorica, Montenegro: https://rm.coe.int/3156-35-iproceeds-assessment-guidelines-for-private-sector-montenegro-/1680726eaf
B. Cybercrime legislation - country profile – Montenegro
C. Law on Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro, No. 33/14 of 04.08.2014: http://www.aspn.gov.me/en/library/zakoni
D. Criminal Code, Official Gazette of Montenegro Nos. 70/2003, 13/2004, 47/3006 and 40/2008: http://www.pravda.gov.me/en/library/zakoni?alphabet=lat&pagerIndex=1
E. The Council of Europe MONEYVAL 2015 Report on Fourth Assessment Visit to Montenegro:https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/16807165d6