iPROCEEDS

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

Version 8 December 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

Serbia

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 the Council of Europe experts, Hein Dries (The Netherlands) 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 all 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 Belgrade, Serbia on 22-23 June 2017, where they met with representatives of several relevant institutions.

1.2.1 Meetings

Meetings were held with the following agencies and institutions[3]:

- The Administration for the Prevention of Money Laundering of the Ministry of Finance – APML;
- The Republic Public Prosecutor's Office – Special Prosecutor for Cybercrime;
- The Ministry of Interior - Cybercrime Unit (MoI);
- The National Bank of Serbia (NBS);
- The Tax Administration – responsible for the supervision of gambling;
- The Association of Serbian Insurers;
- The Serbian Securities and Exchange Commission (SEC);
- The Association of Serbian Banks;
- Money Remittance Providers;
- Internet Payment Providers; and
- The Association of Accountants and Auditors.

In each case, the topics covered during 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.

1.2.2 Research

A desk review of 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.

[3] The link to the outline of the meetings is provided in Appendix A.

- 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 the Prevention of Money Laundering and the Financing of Terrorism (AML/CFT Law)[4], the Criminal Code[5], the APML's updated Directives and Lists of indicators for recognising suspicious transactions related to money laundering and financing of terrorism[6], and the Rulebook on Methodology for implementing requirements in compliance with the AML/CFT Law (hereinafter referred as Rulebook)[7] have been analysed and reviewed. In the assessment provided below, the most recent Council of Europe MONEYVAL Committee mutual evaluation report (MER)[8] on Serbia and other documents related to criminalisation of online fraud and other criminal offences mentioned in the Budapest Convention on Cybercrime have also been taken into account.[9]

1.2.3 Legislation

In Serbia, all criminal offences envisaged under the Budapest Convention on Cybercrime, including the computer-related fraud, are included in the Criminal Code.[10]

The money laundering offence is set out under Article 231 of the Criminal Code and, as regards the predicate offences; it is based on "*all crime*" approach[11]. According to the MONEYVAL 2016 MER on Serbia, the criminal act of money laundering is broadly in line with the relevant AML/CFT international standards.[12]

The reporting of suspicious transactions for all obliged entities is regulated in Paragraph 2 of Article 37 of the AML/CFT Law, which reads as follows:

"(2) The obligor shall furnish the APML with the data laid down in Article 81, paragraph 1 of this Law whenever there are reasons for suspicion of money laundering or terrorism financing with respect to a transaction or customer, before the transaction, and shall indicate, in the report, the time when the transaction is to be carried out. …."

In Paragraphs 3 and 6 of the same article it is also stated:

"(3) The reporting obligation for transactions referred to in paragraph 2 of this Article shall also apply to a planned transaction, irrespective of whether or not it has been carried out.

[4] See Appendix C.
[5] See Appendix D.
[6] See Appendix E.
[7] See Appendix E.
[8] See the MONEYVAL 2016 Fifth Round Evaluation Report on Serbia (https://rm.coe.int/anti-money-laundering-and-counter-terrorist-financing-measures-serbia-/1680715fdb).
[9] See the Council of Europe Cybercrime legislation - country profile, Serbia (Appendix B).
[10] Computer fraud is criminalized in Article 301 of the Criminal Code.
[11] This means that all criminal offences, including cybercrime related offences, are predicate offences for money laundering.
[12] See the MONEYVAL 2016 Fifth Round Evaluation Report on Serbia, pages 28, 150 and 151.

(6) The obligor shall send the data referred to in paragraphs 1 to 4 of this Article in a procedure prescribed by the Minister".

In this regard, it is worth mentioning that the AML/CFT Law in Article 2, paragraph 1 provides for a separate definition of the money laundering for the purposes of the preventive measures, which is broader than the money laundering definition in the Criminal Code, and includes (amongst others) possession of funds that are proceeds of a criminal offence (without any knowledge required by the person).

The analysis of these provisions shows that they are compliant with the Financial Action Task Force (FATF) Recommendation 20[13] 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[14], which require reporting to the Financial Intelligence Unit any suspicion that the funds are the proceeds of criminal activity, or are related to terrorist financing. As it can be seen from the above, paragraph 2 of Article 37 should be read in conjunction with paragraph 1 of Article 2 of the AML/CFT Law. This has been recognised also by the MONEYVAL in its 2016 MER on Serbia, where Serbia was rated "*Compliant*" with the FATF Recommendation 20.[15]

The AML/CFT Law in paragraph 1 of Article 50 requires that the obliged entities shall develop a list of indicators for recognising persons and transactions with respect to which there are reasons for suspicion of money laundering or terrorist financing. In paragraph 2 of the same article it is stated that when developing the list of indicators, the obliged entities shall take into account the following:

- complexity and extent of executed transactions,
- unusual transaction execution patterns,
- value of or links between transactions which have no justifiable purpose in economic or legal terms, or transactions which are inconsistent or disproportionate to a normal, or expected, business operations of the customer, and
- other circumstances linked to the status or any other characteristics of the customer.

The law further determines (paragraph 3 of Article 50) that the obliged entities must apply the list of indicators when determining whether there are reasons for suspicion of money laundering or terrorist financing. Moreover, the law stipulates (paragraph 4 of Article 50) that the Minister of Finance may adopt a list of mandatory indicators which the obliged entities will have to add to their own lists. The list of indicators shall be developed in cooperation with all AML/CFT supervisory bodies (see Articles 51 and 82 of the AML/CFT Law) and according to the law (see Article 65, paragraph 1, point 3 of the AML/CFT Law) the APML shall also take part in their development.

---

[13] See the FATF 2012 Forty Recommendations (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html).

[14] 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).

[15] See the MONEYVAL 2016 Fifth Round Evaluation Report on Serbia, page 176.

With regard to the use of the indicators, the Rulebook provides some additional clarifications. In Article 23 of the Rulebook it stated that when developing the list of indicators, the obliged entities shall also include the indicators published on the APML's website.

Based on these provisions, the AMLP in 2014 and 2015 adopted 17 directives and lists of indicators for recognising suspicious transactions and published them on its website.[16] With the exception of the list of indicators for organisers of special games of chance in casinos, all other lists of indicators are not presented in any structured way, e.g., per client, transaction, product or service.

It is clear from the above that the national legislative framework already requires the obliged entities to report to APML any suspicion of any criminal activity or attempted criminal activity. On the recipient's side, the AML/CFT Law formally limits all powers of the APML[17], so that they can only be used for the purpose of preventing money laundering and terrorist financing. However, due to the broad definition of money laundering in Article 2 of the AML/CFT Law, it seems that the APML can use its powers also when dealing with cases of online fraud, including the attempted online fraud, and other cybercrime, where there is no suspicion of money laundering as defined by the Criminal Code.

2 Typologies and Selected Case Studies

As mentioned in Section 1.1, meetings were held with various agencies to understand:

- 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.

This section provides a discussion of the typologies, case studies and other observations made by the experts during those meetings.

[16] See http://www.apml.gov.rs/eng49/dir/Indicators.html. In 2014 and 2015 the APML updated the indicators for money laundering, while in 2015 the terrorist financing indicators were issued for the first time.

[17] Such as for example the power to temporary suspend a suspicious transaction (Article 56), to order the monitoring of customer's financial transactions (Article 57), to send its reports to the competent state bodies (Article 59) and to provide feedback to the obliged entities (Article 60).

2.1 Administration for the Prevention of Money Laundering - APML

APML issues the indicators that were developed for ML/TF in Serbia. In practice, the following money laundering related indicators are mostly used in the STRs that were reported by banks and remittance providers:

- a general indicator, e.g., "based on experience of the AML compliance officer a transaction seems to be suspicious";
- (structured) transactions in cash below the reporting threshold; and
- the client's transaction is not connected with his/her usual business activity.

Most obligors have more extended indicators than the prescribed minimum set. When they report, then they refer to a mandatory indicator, however. Due to the prevalence of tax fraud, cash deposits by the owners of a firm are also an indicator that is frequently used.

In 2016 the APML received 661 STRs from banks and 1.793 STRs from the remittance services. Attempted transactions are part of these numbers. Cybercrime is not reported often. There is only one case that can be recalled by the APML representative.

Example case 1: Use of remittance service for Bitcoins

- A national of Serbia would receive money via remittance services.
- The amount, although significant, was below the reporting threshold (€ 12k vs € 15k)
- Money was received from multiple countries of origin (e.g., Italy, UK, Malta…).
- Upon withdrawing the customer noted that he is using the money to buy Bitcoins for a friend.
- This is not a type of case that is seen frequently – so far.

Cybercrime is not a common issue for the APML. They did not receive any requests from the prosecution, MoI or foreign counterpart FIUs related to cybercrime. Tax fraud and abuse of office are the main predicate offences they see. There were some indications that there was ID theft linked to documents and ID forgeries, but this was limited in scale.

Virtual currencies are not yet regulated in Serbia. E-banking and M-banking are used as is PayPal. M-Banking is by far the most important electronic product but it attracts low fraud rates. PayPal operates in Serbia in accordance with an exception in the Law on Foreign Exchange Operations, the application of which was sanctioned by the National Bank of Serbia. APML did not receive any STRs related to these products/services/transaction channels.

In practice, the Serbian policy is that the prosecutor will freeze transactions first, since he has less risk of being responsible for potential damages if the order turns out to be unlawful.

The APML dealt with a credit card fraud once, but this was also more of an incidental case.

Example case 2: Credit card fraud

- In 2015 a credit card fraud was reported by a Serbian Bank.
- The reason that it was reported to the APML seemed spurious, and the staff present at the meeting had limited further details.
- The report was also made to MoI and prosecution, which is a standard practice in such cases.

2.2 The Republic Public Prosecutor's Office – Special Prosecutor for Cybercrime and the Ministry of the Interior - Cybercrime Unit (MoI)

Cybercrime is the third largest proceeds generating crime in Serbia, yet it has not been assessed as such during the 2013 national ML/TF risk assessment. So far, the Special Prosecutor's Office only received one or two reports from the APML, and these reports did not lead to investigation. They did not receive any requests from abroad related to cybercrime.

The Special Prosecutor's Office identified a number of relevant cybercrime typologies in Serbia.

Typology 1: Credit card fraud

- Cards (or card data, so called BIN data) are usually bought from other countries.
- Often the proceeds are laundered and perused in Serbia.
- ATM skimming may also be used.
- Skimming is often related to Romanian and Bulgarian criminal groups.
- In one case, a person used a stolen card for gambling and spent in excess of 1M EUR before this has been detected.

Typology 2: Business Email Compromise (BEC)

- This is a very common phenomenon.
- The fraud is usually committed by foreign criminals.
- Social engineering is used to persuade Serbian companies, and sometimes even governmental institutions, to make payments for regular supplies to a different bank account.
- Email and communications are hacked using any available means.
- Email is used to demand a change of IBAN/account for the payee or to send a forged invoice.
- The email communications are monitored to make sure timing of the IBAN change request or forged invoice is very believable.
- Weekends and holidays are used to delay bank's ability to respond and detect the fraud. Fraudulent transactions are timed just before.
- Fraud amounts often exceed € 100k.

Example case: BEC fraud

- The suspect, Serbian citizen, organised a credit card fraud in Montenegro and used money mules in Serbia.
- Three foreign companies were defrauded, and each lost around 500.000 EUR. The money mules - Serbian companies - took their fees and ordered the remaining amounts to be sent to foreign accounts in Switzerland, Romania and Montenegro from where it was eventually disbursed to China.

- Money mules were used in Serbia. They would take a small fee.
- The bank accounts of these Serbian companies were dormant for a long time before carrying out these transactions, yet the banks did not report any STRs to the APML.

In relation to BEC the Special Prosecutor's Office highlighted that it is quite easy to defraud a company and move the related funds. In relation to tracing funds, communications between authorities is not good enough. A faster and more coordinated response is needed. Lastly, in many cases, courts are not easily applying the temporary measures, and seem focused on the predicate offence. Companies, also, need to be more aware to prevent this fraud from happening in the first place.

Typology 3: Money laundering and airline ticket fraud

A specific case involved (online and POS based) sales of airline tickets.

- A company is set up in Serbia by criminals.
- It purchases an existing travel agent with access to online booking systems and a credit line at a major airline.
- The criminals issue tickets to retail customers using a POS terminal (delivered and installed at locations rented specifically to commit fraud) and using the bought company as a front for the sales, amongst others.
- Payments and sales can also be made online using (stolen) cards.
- The tickets are paid by the customers (travellers), and issued by the airline.
- The tickets were payable to the airline by the front company but this company is deliberately bankrupted, sold or abandoned.
- The money is taken from this company and laundered (in existing cases: though Turkey and Israel).
- The airline is thus left with a large amount of unpaid, yet issued tickets.
- Money mules – long dormant Serbian companies - transferred the money to Israel and Turkey where it was not easy to trace further, partly due to lack of cooperation.
- The perpetrators used the e-banking and carry out their transactions over the weekend.
- Sales were significantly higher than usual, but often remain undetected by the airline until it is too late to recover the funds.

This fraud was detected twice, victimising two different airlines.

Typology 4: Extortion of businesses

In some cases, extortion is executed via online channels, using information gathered in attacks on companies.

- A major company with valuable information (such as designs or content – like movies) is hacked or falls victim to a disgruntled employee that stole data.
- Examples are source code of software or pre-premiere movies and series.
- The suspect will then ask the company to pay a ransom unless the data or information is released to the public online.
- Often, samples of the information are released to the public or the company in order to substantiate the claims of the suspects.
- Ransom payment is demanded and is frequently asked in Bitcoins or online payment methods.

The Special Prosecutor's Office raised a number of important issues in relation to similar cases:

- The principle of many international instruments is that money is frozen in the country where it is found. The Warsaw Convention makes it possible to send the money to the country of the victims.
- The UK has a threshold in place in relation to fraud cases – they do not provide intelligence unless a threshold value for the fraud is met. This causes problems.
- Banks do not report cybercrime related to banking systems. They appear to rather take the loss. This means that no effective prosecution can take place for severe cases of cybercrime.
  The banks' onboarding procedure should allow for sufficient information to be gathered allowing automated fraud detection. The expected turnover (inflow), type of business and other details can be used to effectively detect potential fraud in software.

2.3 The National Bank of Serbia - NBS

The NBS is the supervisory authority and regulator responsible for banks, payment institutions (including electronic money providers) and financial leasing. In accordance with the the Law on Prevention of Money Laundering and the Financing of Terrorism, NBS also supervises insurance companies, insurance brokerage companies, insurance agency companies, insurance agents (with a license to perform life insurance business) and voluntary pension fund management companies as well.[18] Electronic money was first licensed in 2015, and only one license was issued so far.

PayPal is active in Serbia and conducts international, e-commerce related transactions. The regime it operates under, is that of an "electronic money institution from a third country". This regime is in accordance with the Law on Foreign Exchange Operations.[19] The regime allows for it to provide payment services without being a licensee under the Law on Payment Services.[20] Under this regime PayPal does not provide for transactions between residents, but only for cross-border (e-commerce related) transactions.[21]

Most cases of fraud and cybercrime are expected to be reported to the MoI rather than to the NBS or APML, especially when large amounts are concerned. NBS, as a consequence, do not have much insight into fraud and related phenomena directly nor do they develop policy in this area. Also, Visa and MasterCard do not issue credit cards

[18] Law on Prevention of Money Laundering and the Financing of Terrorism RS Official Gazette, Nos 20/2009, 72/2009, 91/2010 and 139/2014

[19] Art 32 of the Law on Foreign Exchange Operations provides that "Residents may perform international payment transactions also through an electronic money issuer – for the purpose of making payments and collections under electronic purchase/sale of goods and services."

[20] Law on Payment Services (2015): RS Official Gazette, No 139/2014.

[21] Law on Foreign Exchange Operations: RS Official Gazette, No. 62/2006 and amendments and supplements to that Law published in the RS Official Gazette, No 31/2011, 119/2012 and 139/2014.

in Serbia directly (another regular source of fraud) – all credit cards are issued by commercial banks. NBS organizes a local payment card scheme – DinaCard which is used (and issued) by commercial banks. According to NBS, the organizers of payment cards are not the AML/CFT obligors in Serbia, instead the obligations lie with the commercial banks that officially issue the card (using the services of third parties).

AML and CFT functions are supported by software in most of the Serbian banks (all but one). However, only half of the banks have implemented a significant amount of indicators in this software, however. There are no specific cybercrime indicators, yet most banks do have a list of 5 to 10 more indicators for ML/FT next to the mandatory indicators issued by APML. It is believed that these are not related to cybercrime however. The NBS recently asked for a list of these extra indicators, but this information was not available during the meeting.

Serbia has adopted a Decision on Minimum Information System Management Standards for Financial Institutions (RS Official Gazette, No. 23/2013, 113/2013 and 2/2017) by which the Guidelines on the security of internet payments as issued by the EBA have been fully implemented. Moreover, two-factor authentication has been a mandatory requirement for payment service providers providing online payment services since 2011.

Officially, security incidents should be reported to NBS in case of major breaches that interrupt the functioning of the banking system. NBS has a special department that deals with IT security and banks' oversight. So far, however, no major incidents were reported directly, but rather a yearly questionnaire is used to research the current state of play and to send detailed information on trends and emerging threats to NBS (of less intrusive nature). In 2016, through this annual report, banks reported the following cybercrime related incidents:

- 14 incidents of ransomware;
- 3 identity thefts;
- 16 phishing attacks; and
- 4 DDoS attacks.

None of these had significant impact or caused financial loss. It is believed that the number of incidents reported is low and that there is significant underreporting of security incidents.

The IT supervision department is currently working on security guidelines for banks, also in relation to incident reporting. At the same time, they are negotiating to set up a CERT for financial institutions. Serbia currently has a CERT in MoI and a national CERT in the telecommunications regulator; neither are perceived to be easily accessible for banks.

2.4 The Tax Administration

The Tax Administration in the Ministry of Finance is responsible for the AML/CFT supervision in the gaming and exchange offices sectors in Serbia. The provision of these services is subject to license conditions. In practice, the AML/CFT requirements

are not part of their oversight, as this is left to the APML according to Article 124 of the Law on Games of Chance. This causes a significant dilemma and issues in the supervisory regime. In the new draft AML/CFT law this issue should be resolved, and lawmakers have been alerted to the issue.

There are 12 providers of games of chance via Internet (11 are special – meaning that they offer betting or specific games of chance online only, and one is a classical operator – the Serbian Lottery, which has an online presence). All payments in this sector have to be carried out through the bank accounts. Moreover, the providers should keep their software and hardware in Serbia. Transactions with non-registered providers are prohibited. The Tax Administration has direct access to the transaction details on these platforms. They expect to extend this access to "brick and mortar" gambling operations soon.

One indicator for suspicion listed in the indicators for gambling is the "hiding of IP address". This indicator stems from a period when the Serbian Lottery still had the monopoly on online gambling but is not actively used in practice. Currently they require that all players are identified. Foreign websites offering gambling are not easily blocked. Instead the Tax Administration prohibits transactions involving non-registered providers.

The Tax Administration is not aware of any online frauds or money laundering cases in their respective sectors.

2.5 The Association of Serbian Insurers

The Serbian insurance sector has little experience with cybercrime. The only incidents, so far, were related to phishing emails. One company was affected by a recent ransomware attack (WannaCry).

Life insurance is offered by 15 to 20 companies in the market. The average premium is between €150-200 and a yearly maximum of €15.000. Only one company sells life insurance with an investment component, yet this product is rarely sold. Premiums can only be paid by bank transfer.
The current AML/CFT legislation puts in place a threshold of €100 premium per month: above this premium, clients are perceived a high-risk by default. Currently around 10% of customers pay premiums over the threshold. The new AML/CFT law will put in place a higher threshold. The delegates believe that age is also an important factor, in addition to the total sum payable, the monthly premium and any unusual transactions against the policy and details thereof.

The sector reported 3 STRs in the last year, all of which were related to foreign citizens using forged IDs, and in one case, a high-risk client.

In life insurance no transactions are done online (although this would be allowed in some cases), and most companies have a strict policy to only allow face-to-face transactions in relation to changes to insurance policies. Websites are not used for managing products, although in some other areas online transactions are more common (such as travel and car insurance).

IT security is regulated through a separate bylaw. Most insurers have a regular audit cycle that involves penetration testing of their IT infrastructure. There has been one incident of a domain name takeover in the sector. Few details were available.

2.6 The Serbian Securities and Exchange Commission (SEC)

The Serbian capital market is relatively small and represents only 1% of the financial market. Bonds are more frequently traded than shares and transactions on the exchange are conducted through special bank accounts that may be opened for trading on the Serbian capital market with all Serbian banks. Clients may have more than one such account - at separate banks, for example.

The market consists of 25 individual brokerage houses and 11 brokerage houses that are part of banks. There are 4 investment management companies and around 12 investment funds. Banks and brokers are reporting entities under the AML/CFT legislation; the Stock Exchange itself is not, however. Trading is done electronically via a central platform, operated by the exchange.

Money laundering and terrorist financing detection is not automated; instead, client risk is assessed on the basis of a standardised questionnaire that results in a score for each client. Traditional BEC fraud is less of a risk, also due to the special accounts that are used for trading. Email correspondence with brokers is not uncommon however. Adequate IT security is part of the licensing conditions for broker/dealers. There were no incidents of hacking or security breaches, so far.

They identified several cases of market manipulation that were all reported to the Prosecutor’s Office. Insider trading only recently became a criminal offence and no such case was detected up to now.

2.7 The Association of Serbian Banks

In the last month banks in Serbia detected ten online frauds. Banks have set up a fraud forum in the Banking Association to share information about such cases and, where possible, block the funds if they are still within the country. So far, blocking of fraudulent transactions was successful in around 70 % of cases. In these cases, banks usually instruct the clients to report to the police/prosecutors and they do not report by themselves.

Communication between the banks and their clients is rarely done via e-mail. In fact, clients prefer to use e-banking. This presents some risks, however.

Example case: eBanking – account takeover

- In one case, a bank client's PC was hacked and taken over by cybercriminals. E-banking is done using smartcards readers (and cards) attached to the computer.
- The client had left his smartcard in the reader – which was still attached to the PC.
- Using his credentials, the criminals were able to transfer money from his account.
- Money was then sent to mule accounts and after a fee was deducted, money was transferred further.

Only three banks put all client data collected during the onboarding procedure in their IT systems used for ML/TF and fraud detection. Internet related data, such as IP address data and other identifiers, are usually not used as an indicator for identifying suspicious transactions. In practice, these types of data are used in detecting credit card fraud only. The "know your customer" (KYC) procedures and customer due diligence (CDD) practises differ significantly, per bank.

The Serbian Data Protection Authority (DPA) also makes exchanging of fraud data and related personal details difficult. In one case, they halted the development of a central account register, which was to be set up by the Association of Serbian Banks to detect mule accounts more efficiently. Although Article 75 of the AML/CFT Law allows for data to be exchanged between banks for fraud prevention purposes, the DPA did not recognise the need for fraud prevention as a valid ground for processing. It can be queried of this is a correct interpretation of both the AML/CFT legislation and the data protection legislation.

In Serbia, the Payoneer card (a US based prepaid MasterCard) is on the rise. Especially start-ups and freelancers are using this card linked to a PayPal account.

Referring to BEC cases the Banking Association noted that there are two ways in which email can be abused. In some cases, the criminals impersonate a supplier, and initiate an IBAN account change, using social engineering/impersonation of the supplier. In other cases, criminals directly place orders with the bank, which is only possible in those cases where banks take orders by email.

2.8 Money Remittance Providers

Western Union (WU) covers 99% of money remittance market in Serbia. Tenfore is their largest agent and covers the entire territory. Most transactions (90%) are inbound and only in 10% of cases is money sent out. Most inbound transactions come from Germany, USA, Austria and Switzerland, where the Serbian diaspora mostly leaves. Outbound transactions are mainly directed to the former Yugoslav countries. All senders and receivers are identified and assessed for client risk. ID requirements for EU and Serbian nationals are lighter, meaning they are allowed to transact using the national ID cards, rather than passports, which is the standard for identification of all others.

Cybercrime is not common on the WU service in Serbia. Most cases revolve around e-commerce and non-delivery or non-conformity of items purchased. One case in Germany involved offering a € 10.000 worth Ferrari and cheap houses in Italy. They also identified cases related to the UK and Turkey. Perpetrators used phishing to client's friends (urgent request for money – whilst travelling) and were then asking for money. On average, they identify 2-3 attempted frauds every month, mostly linked with Nigeria.

Example case: Online purchase fraud

- A client is shown an unusually cheap car online – yet proceeds to contact the seller.
- The seller further entices the buyer and presents reasons for the deal to be valid.
- The seller then asks to be paid in advance by way of a WU transfer.
- Once the money is sent (and received) all contact is lost.

Most STRs relate to connected transactions that exceed the reporting limit of € 15.000. Although there is no legal standard for the period of connected transactions, WU itself uses a period of 31 days for transactions to be considered connected.

WU has a limit of $ 7.500 per transaction per person. In Serbia, a further limit of € 10.000 is applied per person per month. The average transaction is in the order of € 300.

Apart from the indicators specifically designed for remittance services and issued by APML, WU also uses local indicators that are applied before the transaction is sent to the global WU system. If a specific risk exists, some transactions may be postponed, in some cases also until the potential receiver has contacted WU to provide more information. In the latter case, the sender has to come back and confirm the transaction afterwards. This is done mostly for unusual transactions, and is often triggered based on the sender country. Two AML/CFT compliance officers are responsible for these transactions, and clear them, rather than the front desk agents.

Attempted frauds are also detected, but usually these are not reported to either the police or APML. They rather put the related information of the sender or receiver on a blacklist, preventing them to conduct further transactions. WU actively prevents cashing out of Bitcoins through their network and block the related parties as well. In cases of fraud even pending transactions are not paid out.

WU is working to allow credit card payment at the POS terminals, although the current interchange fees are too high for them to proceed. They are also working on becoming a local partner to Payoneer.

2.9 Internet Payment Providers

Company Limundo runs a payment, e-commerce and classified ads (Limundo Grad) platform in Serbia. They are not strictly a payment provider, but rather provide a platform for transactions that is comparable, internationally to eBay and/or Amazon. They provide escrow services for transactions, although the majority of transactions are paid for through cash payment on delivery. The average transaction is € 10, a maximum of € 200 is imposed on COD payments in Serbia. On the platform, the seller and buyer agree payment methods, so there is a potential for several, more money laundering-prone payment methods, such as virtual currencies or PayPal to be used.

Limundo is regulated by the Ministry of Trade, Telecommunication and Tourism and is not an obliged entity under the Serbian AML/CFT legislation. As a website, they have built an extensive fraud detection platform that includes reporting functionalities to the MoI.

Their detection is based on many data points. They detect stolen images (images that were grabbed from the Internet (which indicates that the seller is not in possession of the object), device ID, IP address and several other indicators.

Often pictures are taken from other websites in "the former Yugoslav Republic of Macedonia" or Bulgaria. Another important indicator is account age. Fraudsters are faster to use an account and display more activity in a short time, than regular users. Certain patterns are used to detect fraud too, related to age groups (age of users), for example. An 80-year-old selling an iPhone is suspicious. The system also triggers on high value sales (> €400) or high-volume traders.

Domestic (e-money) payment providers have a limited presence in the Serbian market. Only one provider has a license. The Foreign Exchange Law only allows for international players to operate in the Serbian market in relation to international (e-commerce) payments.

2.10 The Association of Accountants and Auditors

These sectors only use the APML indicators for suspicious transactions and they believe the current indicators are not fully reflecting the specifics of these sectors. In Serbia, there is no basic legislation in place regulating the businesses of accountants and tax advisors. In practice, the accountants do report STRs to the APML, but usually their STRs are of a low quality.

The Association is active in education of their members on ML/TF and cybercrime related issues.

Example case – BEC fraud:

- One of the Association's members had an issue with a client that fell for a BEC fraud.
- The client had a bank account with e-banking in Greece.
- A payment was made from this account to an account that was changed upon a supplier's request on a Friday afternoon.
- The money was diverted to Croatia rather than the actual suppliers account.
- The client then asked their accountant for advice.
- The client contacted Croatian police directly, yet a solution was not reached.

The Association emphasises that more attention could be paid to crime proceeds in relation to STR reporting. It is currently treated mostly as something that is strictly related to money laundering.

3 Indicators

As mentioned above, the indicators for suspicious transactions are provided in the Directives and Lists of Indicators published by the APML.[22] The analysis of these documents shows that apart from one indicator related to terrorist financing and two indicators related to organisers of games of chance operated on the Internet there are no other cybercrime specific indicators included in the current lists. This means that the existing 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 indicators have been identified that can also assist obliged entities in preventing/detecting online frauds[23] and online money laundering. These indicators can be divided into those that apply to the suspect's account/transactions or to suspect's and victim's accounts/transactions.[24]

a) Indicators applying to the suspect's account:

- Cash payments or non-cash income to accounts of natural persons and a transfer of money to the benefit of third parties (legal and natural persons) in the country and abroad, when it can be concluded that such transactions are not in line with usual or expected activities of a client (June 2014 Directive, Indicators for Banks, Point 1).
- Transactions on basis of trade in services (e.g. consulting, marketing, accounting, intermediation and other) which are difficult to determine the market price for and are inconsistent with expected or usual activities of the client (June 2014 Directive, Indicators for Banks, Point 9).
- Frequent transactions in high amounts with persons from countries which do not implement AML/CFT standards, or from countries which have strict bank secrecy provisions (June 2014 Directive, Indicators for Banks, Point 10).

[22] Some lists of indicators published on the APML website do not contain the date of adoption/publishing and it is therefore difficult to assess which of the lists of indicators applying to the same sectors are actually in force.
[23] CEO/BEC frauds in particular.
[24] No indicators were identified that would only apply to the victim's account/transactions.

- Situations in which a client has had "passive" (inactive) accounts for a while, which suddenly record an income inconsistent with the client's usual or expected business activities and from which the client withdraws or further transfers money (June 2014 Directive, Indicators for Banks, Point 18).
- Opening and closing of bank accounts in a short time period, especially when combined with a transfer of funds to an account opened in another bank (June 2014 Directive, Indicators for Banks, Point 19).
- When opening an account, a client does not want to provide necessary data, or provides falsified and incomplete documentation difficult to be verified. Moreover, when carrying out a transaction, a client is reluctant to provide the requested data on the beneficiary of the transfer, or changes the beneficiary on the transaction order; a client provides too much explanation on the legality of the transaction or enquires about the system of control of banks and regulations in the AML area (June 2014 Directive, Indicators for Banks, Point 25).
- Frequent withdrawals in high amounts on ATMs in high risk countries (June 2014 Directive, Indicators for Banks, Point 29).
- The client has bad reputation, he is known for having been involved in illicit activities or his past cannot be verified (September 2015 Directive, Indicators for Broker-dealers and Authorised Banks, Point 6).
- A client with bad reputation or with assets of dubious source is known to be using virtual currencies, for example bitcoin, litecoin, or is using alternative remittance systems (for example, hawala, hundi) in order to avoid regular financial channels (March 2015 Directive, Indicators for Terrorist Financing, Point 16).

c) <u>Indicators applying to both victim's and suspect's accounts:</u>

- Deposits (cash and non-cash) to accounts of legal persons, followed by a transfer from the accounts of the legal persons to accounts of natural persons, withdrawn in cash immediately or shortly after they are received, with no economic or other logical justifiability (June 2014 Directive, Indicators for Banks, Point 3).
- A client disposes of funds on bank accounts, or carries out transactions on various bases, inconsistent with the client's usual activities or profile (June 2014 Directive, Indicators for Banks, Point 5).
- The originator or beneficiary of a bank wire transfer is a citizen of a country which does not implement AML/CFT regulations (June 2014 Directive, Indicators for Banks, Point 14).
- Transactions assessed by a bank staff as unusual for a client's normal activities, based on the staff experience (June 2014 Directive, Indicators for Banks, Point 30).
- Players possess credit cards issued in offshore destinations or in countries that do not comply with standards against money laundering and terrorist financing (the black list) (List of Indicators for Organizers of games of chance operated on the Internet, Telephone or in another manner using telecommunication networks, Point 1).

  Organiser of the games has some information that the player hides their IP address (List of Indicators for Organizers of games of chance operated on the Internet, Telephone or in another manner using telecommunication networks, Point 4).

4 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, APML 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.

4.1 Legal/Policy Recommendations

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

- The AML/CFT Law in paragraph 4 of Article 50 authorises the Minister of Finance to adopt a list of mandatory indicators which the obliged entities will have to add to their own lists and also requires that the APML takes part in their development (Article 65, paragraph 1, point 3). In reality, all lists of indicators were adopted by the APML. It is therefore recommended to whether amend the AML/CFT Law and authorise the APML to adopt the mandatory indicators or change the current practice, so that the lists of indicators would be adopted by the Minister of Finance (based on the APML's proposal).
- The authorities should consider including in the list of indicators also indicators related to other major proceeds generating criminal offences (e.g., predicate offences for money laundering). In the development of these indicators, in addition to the APML and AML/CFT supervisory authorities, also the competent law enforcement authorities should be involved.
- It is recommended to better structure the list of indicators so that they would be presented, for example, per client, transaction, product, services, transaction channel, geographical risk, etc.
- The APML website should only contain the updated versions of indicators for recognising suspicious transactions that are currently in force.
- The banks and other obliged entities should be instructed to report their suspicion of CEO/BEC frauds or attempted frauds simultaneously to the APML and the competent police authority/prosecutor to ensure that these authorities can promptly take all the necessary measures within the scope of their powers.

  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.

4.2 Indicators

This section presents examples of additional indicators for prevention and detection of online frauds and money laundering that the APML and/or other competent authorities may wish to consider including in the list of indicators for suspicious transactions. In this regard, the authorities may wish to use the structure of the list of indicators for

suspicious transactions presented below or include an additional section in the current lists with indicators that will only target the online fraud, other cybercrime offences and related money laundering.

General indicators:

- The transaction is related to buying or selling the virtual currency (e.g., Bitcoins, Litecoin, Ethereum, Zcash).[25]
- The transaction is related to transfer of winnings from an online gambling platform.
- The client requests a transaction to be carried out urgently or requests that it should be treated as confidential.

Indicators related to bank accounts:

- 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 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.

Indicators related to corporate 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.

[25] In the APML Directive that provides indicators for suspicious transactions related to terrorist financing there is already an indicator (see point 16) that deals with virtual currencies. However, this indicator is only related to terrorist financing and includes some additional criteria and conditions.

Indicators related to geographical risk:

- The transaction involves a country which 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.

5 Appendixes

A. Agenda of the assessment mission of guidelines to prevent and detect/identify online crime proceeds, 22 -23 June 2017, Belgrade, Serbia: https://rm.coe.int/3156-35-assessment-mission-guidelines-private-sector-serbia/1680729e05
B. Cybercrime legislation - country profile – Serbia
C. Law on the Prevention of Money Laundering and the Financing of Terrorism, Official Gazette of the Republic of Serbia, Nos. 20/2009, 72/2009, 91/2010 and 139/2014: http://www.apml.gov.rs/eng46/dir/Laws.html
D. Criminal Code, Official Gazette of the Republic of Serbia, Nos. 85/2005, 88/2005, and 107/2005: https://www.mpravde.gov.rs/en/tekst/1701/criminal-matter.php
E. APML's Directives and Lists of Indicators for Recognizing Suspicious Transactions related to Money Laundering and Financing of Terrorism: http://www.apml. gov.rs/eng49/dir/Indicators.html
F. Rulebook on Methodology for implementing requirements in compliance with the AML/CFT Law, Official Gazette of the Republic of Serbia, Nos. 7/210 and 41/2011: http://www.apml.gov.rs/eng/file/?conid=626