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

"The former Yugoslav Republic of Macedonia"

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 service providers, ranging from bank transfers, cash withdrawals/deposits, the use of digital/electronic currencies to money mules and money remitting services.[1] Often the chain of electronic transactions is "broken" by cash operations performed physically by money mules, followed, sometimes, by the use of a traditional payment services. If the respective payment service is integrated with an Internet payment service provider, 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 require the inclusion of a wide range of stakeholders. 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. Online criminality can be significantly reduced by raising awareness among the potential victims. However, 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 recognize 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-Ziekenheiner (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

[1] See MONEYVAL 2012 Research Report on criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction, pages 6 and 38 (https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a).
[2] See FATF Recommendation 34.

environment. The report is also aiming to address some legal and policy issues 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 Skopje, "the former Yugoslav Republic of Macedonia" on 15-16 June 2017, where they met with representatives of several relevant institutions.[3]

1.2.1 Meetings

Meetings were held with the following agencies:

- Financial Intelligence Office - FIO;
- Computer Crime and Digital Forensics Sector, Ministry of Interior;
- The National Bank;
- The Securities and Exchange Commission;
- The Insurance Supervision Agency;
- The Notaries Association;
- The Bar Association;
- Internet payments service provider – company Casys;
- The Western Union agent – company Unija Finansiska;
- The Grand Casino; and
- Representatives of several banks and the Banking Association.

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 all relevant legislation has been conducted with the following objectives:

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

- 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; and
- 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 relevant provisions of the Law on Prevention of Money Laundering and Financing of Terrorism (AML/CFT Law)[4] and the FIO List of indicators for determining suspicious transactions for money laundering and terrorist financing have been analysed and reviewed. In the assessment provided below, the most recent Council of Europe MONEYVAL Committee mutual evaluation report (MER)[5] on "the former Yugoslav Republic of Macedonia" 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.[6]

2 Legislation

In "the former Yugoslav Republic of Macedonia", all criminal offences envisaged under the Budapest Convention on Cybercrime, including the computer-related fraud[7], are included in the Criminal Code.[8] The criminal offence of money laundering (Article 273 of the Criminal Code) is based on *"all crime"* approach[9] and is to a large extent criminalised in compliance with the FATF 40 Recommendations and other relevant AML/CFT international standards.

The reporting of suspicious transactions (STRs) for all obliged entities is regulated in paragraph 1 of Article 30 of the AML/CFT Law, which reads as follows:

"The entities[10] shall be obliged to submit the collected data, information and documents to the Office[11] in the following cases:

a) when they have suspicions and grounds to suspect that:
- it has been or was performed money laundering and/or financing terrorism or there was or there is an attempt for money laundering or financing terrorism, regardless the amount of the transaction;
- the property is a proceed of crime;

---

[4] See Appendix C.
[5] See MONEYVAL 2014 Report on Fourth Assessment Visit to "the former Yugoslav Republic of Macedonia" (https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715adc).
[6] See the Council of Europe Cybercrime legislation - country profile, "The former Yugoslav Republic of Macedonia" (Appendix B).
[7] Computer fraud is provided in Article 251-b of the Criminal Code.
[8] Ibidem.
[9] This means that all criminal offences, including cybercrime related offences, are predicate offences for money laundering.
[10] The list of all obliged entities is provided in Article 3 of the AML/CFT Law.
[11] *"Office"* means the Financial Intelligence Office – FIO.

- the property is related to financing terrorist act, terrorist organization or terrorist or person who finance terrorism; …"

In this regard, it is important to mention also the definitions of terms "*Proceeds of crime*" and "*Property*" that are provided in paragraphs 3 and 5 of Article 2 of the AML/CFT Law:

"Property" shall mean money or other payment instruments, securities, deposits, other property of any kind such as tangible or intangible, movable or immovable, regardless of the manner of acquisition as well as other rights over objects, claims, public and legal documents for ownership and assets in written or electronic form, or instruments that prove the right of ownership or interest for that property."

"Proceeds of crime" shall mean any property or benefit, directly or indirectly, acquired by committing criminal offense. The proceeds of crime shall also include proceeds of criminal offense committed abroad, if at the time it was committed it was determined as a crime by both laws in the state where it was committed and in Republic of Macedonia."

The analysis of these provisions shows that the obliged entities must report to the FIO not only when they suspect that money laundering or terrorist financing has been committed or attempted, but also when they suspect that the property is a proceed of any other crime. It can be therefore concluded that these provisions are fully compliant with the Financial Action Task Force (FATF) Recommendation 20[12] 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[13], which both require obliged entities to report to the Financial Intelligence Unit when they have a suspicion that the funds are the proceeds of criminal activity, or are related to terrorist financing.

The AML/CFT Law in Article 31[14] regulates that the obliged entities should determine their grounds of suspicion based on:

- Immediate information;
- List of indicators for recognising suspicious transactions determined by the FIO, the obliged entities and supervisor bodies;
- The international list of terrorists and terrorist organisations; and
- In accordance with their internal risk assessment.

In paragraph 1 of Article 34 the AML/CFT Law further requires the obliged entities to prepare, inter alia, a programme, which shall contain procedures for recognition of unusual transactions and suspicion for money laundering and financing of terrorism.

---

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

[13] 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).

[14] The same article in paragraph 2 also requires the FIO to update the list of indicators.

According to paragraph 2 of Article 40 of the AML/CFT Law, the list of indicators for risk analysis and recognising suspicious transactions should be prepared by the FIO in cooperation with the obliged entities and their supervisory bodies. Based on these provisions, the FIO drafted, altogether, 20 lists of indicators for all financial institutions and designated non-financial businesses and professions – DNFBPs that are obliged entities under the AML/CFT Law.[15]

It is clear from the above that the national legislative framework requires the obliged entities to report to FIO any suspicion of criminal activity or attempted criminal activity, including the online fraud and other online criminal activity. Nevertheless, it seems that the current lists of indicators issued by the FIO as well as Article 34, paragraph 1, fifth bullet point of the AML/CFT Law are somehow limiting the scope of detecting/reporting of suspicious transactions only to money laundering and terrorist financing.

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

For example, the following provisions of the AML/CFT Law apply to both mentioned situations (e.g., when FIO suspects that money laundering, financing of terrorism or any other criminal offence has been committed):

- Article 40 of the AML/CFT Law which defines all FIO functions;
- Article 81 that distinguishes between two types of documents that FIO shall submit to the competent state authorities: a) a report, when it finds out that there is a suspicion of money laundering or financing of terrorism, and b) a written notification, when it finds out that there is a suspicion of other criminal offences; and
- Article 79 which regulates the FIO authority to request data and information from the obliged entities and state authorities.

On the other hand, the following provisions of the AML/CFT Law apply only to cases, when FIO suspects that money laundering or financing of terrorism was committed:

- Article 82, which regulates the FIO power to order a monitoring of a business relationship; and
- Article 83, which authorises FIO to order a temporary detention of a transaction and to send a request for provisional measures to the competent public prosecutor.

In practice, this means that if, for example, a suspicious transaction related to an attempted online fraud is reported by the bank to FIO, the latter is formally not allowed to suspend it; however, it may send this information and its analysis with a written notification to the competent law enforcement authority/prosecutor. During a

[15] It is worth mentioning that while the list of indicators for banks include indicators for detecting both money laundering and terrorist financing, other lists only refer to money laundering.

desk review, the objectives behind the explained division related to the use of FIO powers remained unclear.

3 Typologies and Selected Case Studies

As mentioned in Section 1.2.1, 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]

3.1 The Financial Intelligence Office, Ministry of Finance

Among the reporting entities, only banks are using software supporting money ML/TF detection. Fraud detection is not automated. A bylaw prescribes the software's minimum functionalities in relation to ML/TF and reporting. When reporting a suspicious transaction, the obliged entities should postpone it for up to 4 hours upon which the FIO may suspend it for another 72 hours pending a freezing order.

Only a limited number of cybercrime cases were dealt with in the FIO and there are no separate statistics for these types of cases. Most cybercrime cases are opened in the FIO based on the requests from the Cybercrime Sector in the Ministry of Interior (usually these are credit card fraud cases), and not based on STRs. The main frauds detected are Business Email Compromises (BECs). The banks usually report BECs to the police or they instruct victims to do so.

During the meeting, the following typologies were discussed:

Typology: BEC

[16] During the meetings with the Securities and Exchange Commission, the Insurance Supervision Agency, the Grand Casino, the Notaries Association and the Bar Association it was found out that no cybercrime or money laundering cases were detected and reported by these sectors. Therefore, the content of the meetings with representatives of these sectors is not presented in the report.

- In one of the earlier BEC cases (2014) the fraud was committed in the United States of America (USA) and proceeds were sent to bank accounts in "the former Yugoslav Republic of Macedonia", which were opened by a non-resident to withdraw money.
- The correspondent bank informed the Macedonian bank that the money was fraudulently obtained and should be sent back. The bank reported an STR since the non-resident was a young man, who received money (€ 80.000 – €140.000 EUR) from abroad and immediately started to withdraw money in cash and ordered money to be sent to China. Furthermore, the client quoted as legal basis for transactions the "gift", "investment", "transfer", and similar. The same pattern then repeated itself at several other banks – where the same person would open the account.
- The time difference was also abused, in order to delay the USA banks opportunity to respond. Although the fraudsters managed to get cash disbursed initially, after several STRs came in, the FIO suspended the remaining transactions.
- The FIO queried the related companies in the USA using open source intelligence (via Internet) and found the sources of the funds to be reputable, well established USA companies. The local accounts would display a small amount as withdrawal (to a local account or person– probably as a fee for the "mule service"). The remainder would be transferred abroad.
- At a later stage, the FIO contacted all banks with an outline of this typology. They asked them to look for non-resident accounts with significant sums of money – by way of indicator. They also sent out a detailed description of the typology.
- Nowadays most cases involve local companies as victims of foreign fraudsters. In most cases the victim suffered a compromised email account and was misled to perform an IBAN code change to an account under the control of criminals.
- The FIO has mandated that IBAN changes are carefully assessed and verified by banks.
- Another issue is that banks also take orders via email, which makes them even more vulnerable as email addresses can be easily spoofed and a fake email order can easily be sent to the victims once the template is known.

The main indicators identified were the following:

- A young non-resident;
- Transactions involved unusually large sums (in the order of $80K-$170K, which is an unusually large amount in the country) and the transfers of these moneys would take place shortly after account opening;
- The client quoted as legal basis for transactions: "transfer, gift, consulting or business investment."

Rigorous onboarding procedure would also help in similar cases. As part of the account opening procedures banks are required to perform customer due diligence (CDD) and assess the likely account usage. If the account is used differently this could also have provided early warning of the abuse of the account. Account monitoring software (ML/TF and fraud detection software) can then be used to identify if the type of transactions performed match the pattern and amount that were expected. The inflow (account turnover) is also a good indicator, if the expected inflow is far exceeding the

expectations this should be analysed. It is important to match the ability of software based detection methods to the questions asked during CDD. Ideally, questions asked should include questions related to the source of wealth.

Another issue is that of feedback on frauds that are detected by the FIO. There is no direct way to communicate lessons learned in one bank to all others directly. In practice, this means that the FIO has to call a meeting to inform banks. Apart from this, phone calls are used to exchange information.

Customer risk classification is implemented using indicators that define when a customer is to be considered high-risk. These indicators are separate from those that that are defined by law and international standards (such as the cases of Politically Exposed Persons - PEPs). According to the FIO they will need improvement however, especially if local PEPs are to be analysed in accordance with the 4th EU AML/CFT Directive.

The general policy is that banks are encouraged to have their own, more extensive indicators and the FIO only issues the mandatory minimum in their guidelines.

The usage of mobile and electronic banking is limited. These services allow for all banking operations and are mainly used by young people.

Virtual currencies are not allowed as products in the financial sector. However, no specific measures or actions were mentioned that would hinder such transactions. The FIO did not receive any STRs related to virtual currencies or PayPal.

3.2 Computer Crime and Digital Forensics Sector, Ministry of Interior

The Computer Crime and Digital Forensics Sector at the Ministry of Interior (MoI) confirmed that most BEC cases are reported to them – more than any other authority. These cases are a trend and yet they do not receive many reports from banks or the FIO about such cases. Instead it is usually the victims that contact them. In such cases the Cybercrime Sector usually immediately contacts the bank (and any correspondent bank – if known) to postpone the transaction. They are also obliged to immediately inform the prosecutor, who leads the criminal investigation.

When money is still in the country, the FIO is contacted to postpone the transaction at the relevant bank. They also contact INTERPOL to check for further intelligence and to notify them. They usually inform the receiving/corresponding bank of an on-going investigation by email. Although the Cybercrime Sector has no powers to postpone transactions yet bank policies may be such that transactions are flagged and/or delayed in order to await a formal response from authorities nonetheless. In the majority of cases (2 out of 3) this policy has the desired effect and the transaction is postponed.

In rare cases, they are informed of a BEC case immediately; this is usually because the bank is suspicious of an IBAN change. On average, they deal with ten BEC cases per

month. The smallest are worth € 13K in losses and the biggest cases can range up to € 120K. More detailed statistics are available but were not supplied.

The aim of the MoI overall – so far – was to focus on prevention. Information was disseminated to the public through the PR Department and MoI website. From the recent experience with these cases the MoI notes that a more stringent policy on IBAN changes or new payee IBANs may be needed, especially when they involve similar supplier names as were previously observed. In many cases only slight changes in supplier details, email addresses or domain names are made. Often the same goes for registered business names. These attacks usually start with a form of phishing after which social engineering is applied and the attack (essentially misinformation) is timed according to the email communication that is observed – thereby maximising chances of success.

According to the MoI, indicators of these frauds could include:

- IBAN changes;
- Transaction timing;
- Suspicious delays in regular inbound transactions; and
- A combination of account age, and age, origin and type of business of the account holder.

It is observed that attempted BEC transactions are also an issue. There is likely a significant grey area where banks and victims are underreporting these.

In relation to other (proceeds generating) cybercrime the following examples were provided:

- In 2014 the Cybercrime Sector, together with the FBI, arrested two residents of "the former Yugoslav Republic of Macedonia" in a DDOS and malware case that included a large botnet that was sold to others. Upon request of the prosecutor the judge eventually confiscated the house, car and bank safe contents. The Cybercrime Sector found evidence of an account in virtual currencies. As they did not have a procedure for seizing virtual currencies, these were unaffected by these measures. Accordingly, 3 months after the suspect's release, he was able to buy both a new apartment and a house.
- Remittance services are sometimes abused in cybercrime. They are frequently used to pay for "underground economy" transactions, such as the purchase of stolen cards. In relation to credit card (and POS) related frauds, Bulgaria, Serbia and Montenegro are observed as countries that play an important role in these crimes.
- There are also many cases of e-commerce fraud, where stolen data is used related to international victims. Services or goods are paid in country and internationally, using stolen credit card data. Transactions with this data can be conducted both at online shops (of which a limited number operate in "the former Yugoslav Republic of Macedonia") or at retail outlets using the data on cloned cards with POS terminals. Recently, these frauds are increasingly targeting sales of services. One measure that was taken was to prohibit the use of foreign cards for the purchase of prepaid credit for mobile phones.

3.3 The National Bank

The National Bank (NB) has an IT Supervision Department established in 2003. Their mandate is based on the Banking Law and several decisions regarding information security of banks. NB applies various international standards in this area, in accordance with international best practise, such as the BS 7799 and ISO 27001/27002 standards. They enforce several policies in relation to IT outsourcing and SWIFT operations. Cybersecurity has been a priority for the last two years. A first requirement for the banks is to have clearly defined responsibilities for IT security. In most banks, the IT security function is part of the operational risk or compliance unit. As regards the reporting of incidents to the NB, only reporting of serious breaches against banking systems is mandatory.

NB is currently trying to develop the indicators for detecting online fraud together with the Banking Association. They have consulted with banks on this matter and are working on a list of 20-30 indicators to detect and prevent cybercrime as part of a risk based approach.

The following specifics related to BEC fraud were reported:

- These cases were first detected in 2014/2015 and are still on-going.
- In all BEC cases, there were changes to a supplier/payee IBAN, usually triggered by social engineering. In most cases the instructions were given to send money to the banks in the UK.
- Even when transactions are found to be suspicious, banks often have a hard time convincing customer of the fact that the new account is false and fraudulent. In some cases, the fraudsters even make a few inbound transactions to establish trust before a large outbound transaction is requested and cashed out.

A potential indicator that was mentioned in discussions was that in many BEC cases the bank account and the company receiving the money are in a different country.

Attacks against the banking system itself are not observed frequently - most attacks consist of targeted DDOS attacks. The following cases were reported in this regard:

- An attack was launched and immediately after a "security" consultant was introduced to the bank to "solve" this issue. This was, in fact, a covert way of extorting the bank.
- Ransomware cases have also been detected - directed against both financial institutions and their clients.

A good deterrent used by some Macedonian banks, especially in cases of Internet banking, was to ask for the title to the transaction (proof of the underlying contract or other documentation) to be attached to the transaction in the online environment. This deters many fraudsters according to the NB. This is not implemented by all banks, however, also because e-banking is considered relatively secure. OTP authentication is mandatory for these channels. For legal persons, a full digital signature is required. M-banking is a new product and is limited to natural persons.

In order to assess the cybersecurity risks, the NB has developed a self-assessment tool that assesses the inherent risk of each product offered. Any new product or technology that is introduced requires the bank to perform a separate risk assessment, using the online self-assessment tool. Security and ML/FT risks are both considered in this assessment. Several requests to introduce new products have been rejected based on this assessment, such as a request related to SMS banking. In some cases, there are thresholds put in place to mitigate the ML/FT risks. The NB is looking to develop a better standard for these, however, also with a view to making these limits mandatory. On the security side, the NB notes that they are missing a banking CERT which makes coordinating security incidents harder.

The Foreign Exchange Act prohibits virtual currencies, but NB believes that banks can execute transactions for buying bitcoins for clients. The NB issued two warnings regarding the risks related to the use of virtual currencies.[17]

PayPal is allowed since 2014, but only for buying, e.g., paying for e-commerce transactions. A limit of € 2.500 per transaction was established for natural persons. Otherwise e-money can be licensed in the country, but no license was yet requested, possibly due to the high capital demands.

The Foreign Exchange Act imposes further limits for natural persons; they may not own foreign securities or hold foreign currency accounts. Only legal persons can have these.

3.4 The Banking Association

The Banking Association (BA) also confirmed the presence of BEC fraud. The following examples were reported:

- A hacker misguided a client regarding an order for electronics. The fraudster represented himself as ASUS (a Taipei based electronics manufacturer) using a similar domain. He then sent an email to change the IBAN for the payment of an order of around € 11.000. The client only realised the mistake after a few weeks and a report was made to the MoI. Although the case was not solved, information was received using SWIFT messages and interbank communication.
- In one bank, many BEC cases were detected. They took measures to enhance monitoring and control on SWIFT payments. One of them is that bank officers in branches actively advise clients to call suppliers and confirm the SWIFT account details (IBAN) via a different channel that can be relied on more (dial-out phone calls for example). The value of the cases detected ranged from € 10.000 to € 100.000, and the trend is up.
- In most BEC cases only an IBAN number change is requested, but sometimes a change in name too. Geographically, receiving countries for fraudulently

[17] In one case, related to OneCoin, a scheme trading in pseudo (fake) cryptocurrency, the NB noted that many transactions were obfuscated by the scheme operators and passed the banking system unharmed.

obtained funds are diverse, but most detected were Poland, The United Kingdom and Spain.
- In some cases, changes of IBAN lead to suspicion in foreign banks. In those cases, transactions are stopped and reported to MoI.

For new clients, banks in the country generally take a static risk approach based on information gathered during onboarding (CDD and KYC). This data is entered in software for ML/TF detection. For high-risk clients, they will ask for additional documentation. Software keeps track of the parameters entered. Most banks use Siren or internally developed software solutions for this purpose.

Other frauds in the banking sector have involved:

- Two cases were related to fake letters of credit and foreign guarantees made out to large amounts. Often these involve banks that do not exist. Fraudsters frequently use contacts details from the international banking department and approach them with foreign letters of credit. In both cases the fraudulent activity was detected by the clients, who spotted the change in the name of the bank.
- The use of fax to forge a SWIFT form. In an example case, a florist was issued a forged fax and email as proof of payment.
- DDOS attacks on e-banking systems. The banks have contacted Telekom, the country's largest ISP/Network to resolve this issue. There seems to be no financial motive for these.
- ATM skimming.

The 3D secure reduced e-commerce fraud in card-not-present scenarios are to a very low level recently.

The most frequently used ML indicators by banks are:

- Cash payments under suspicious circumstances (unemployed customer, large amount).
- Cash withdrawals.
- A lack of documentation or title related to the transaction.
- Transactions of unusually large amounts.
- Transactions involving high-risk countries.

Country risk is also used as an indicator. Banks in the country use the OFAC and FATCA lists as well as their own, internally developed solutions. In one case, a bank chose to use a grey list rather than a blacklist for further protection, meaning that transactions would be monitored yet not prohibited. For example, Bosnia and Herzegovina is grey-listed in this system due to the MONEYVAL evaluation report and FATF follow-up procedures.

Virtual currency related transactions will likely be detected by banks although this is not supported by software yet. The BA is also familiar with PayPal but currently is not aware of any problematic issues related to this payment system.

3.5 Internet Payments Service Providers

Casys is a wholesale card issuer and processor that issues Visa and MasterCard and processes payments for all banks in the country. They also provide settlement for certain local cards. As a third-party issuer, they provide services to and on behalf of all 13 Macedonian banks, and are not seen as an obligor under the AML/CFT legislation. Hence, they do not have any ML/TF indicators and they do not report to the FIO. They are audited by international (USA based) auditors for PCI-DSS compliance.

Suspicious transactions are sent to MasterCard/Visa and they inform banks when fraud is detected. Their contract with MasterCard and Visa requires them to have an AML/CFT department, but suspicious transactions are mainly detected by VISA and MasterCard themselves, however, and not by their systems.

"The former Yugoslav Republic of Macedonia" has a very low credit card fraud percentage partly because they implemented EMV (PIN and Chip) and 3DSecure (verification required in certain e-commerce/non-face-to-face transactions). There are numerous (daily) limits in place such as limits on ATM transactions, PIN retries and card capture policies.

Also, there have not been any major data breaches related to credit cards. OTP authentication (3D Secure) was implemented but only one bank uses this technology currently.

Casys have their own fraud detection solution, which assesses fraud risk based on the following criteria:

- Type of card (debit/credit).
- Type of transaction.
- The daily and monthly limits set.
- Transaction limits.
- Origin or destination (foreign transactions can have different limits).

Analysis and reporting STRs to the FIO is left to the bank. For example, suspicious transactions detected by VISA and Mastercard can be postponed and marked. It is for the bank to clear these transactions based on their own analysis.

Since, according to PCI-DSS, Casys is not allowed to store names of clients of Visa and MasterCard cards, they do not perform any checks on UNSC or other blacklists related to terrorism.

3.6 Money Remittance Providers (Western Union)

"Unija Finansiska" is the largest Western Union agent in "the former Yugoslav Republic of Macedonia". As such they are bound by a contract to implement the Western Union policies to prevent and detect frauds as well as the AML/CTF policies.

Most of their fraud cases are related to purchase of goods via the Internet and the following examples were provided during the meeting:

- The seller is requesting an advance payment, carried out via remittance. After receiving the money, the seller disappears. Western Union actively blocks all such recipients after detecting such frauds.

Employees that execute these transactions receive training, also in detecting suspicious transactions, but only a limited amount of information on the nature of transactions can be derived at the counter. The company claims that employees are not allowed to ask for the nature of the transaction. Only name, address and date of birth of the sender and receiver are registered. Online accounts are not used in the country.

Both the law on Fast Money Transfer[18] and Western Union policy require limits to transactions performed on the service. Western Union allows only one transaction per day, per person. Monthly transactions per person cannot exceed € 2.500. A € 5.000 threshold is applied regarding the receiving of money.

The company uses software to find matches and detect structured transactions, based on sender and receiver information. In this regard, the country risk is also taken into account. For example, Afghanistan, Syria and Iran are currently black-listed and their black list includes additional 20 problematic countries. Another list – the so called grey list - defines countries where transactions are being monitored, such as for example Turkey and Bosnia and Herzegovina. The source of wealth defines the location for this purpose, not the country or physical presence of the sender. Most funds are received from EU countries and sending money is mainly done within the region.

4 Indicators

As mentioned above, the indicators for suspicious transactions related to money laundering were drafted by FIO. The introductory part is only included in the List of indicators for banks, where the objectives and scope of indicators are described as follows:

- This list of indicators is a basis that each bank can supplement, adjust and include its experience in detecting suspicion of money laundering or financing of terrorism;
- This list of indicators is not definite, because there are no (pre)established behaviour schemes in cases of money laundering or financing of terrorism;
- The indicators do not have to be necessarily present. If the bank has other justified suspicions, it should submit the STR.

The lists of indicators are divided into the following categories: i) Common indicators for all entities; and ii) Sectors' specific indicators[19].

[18] Law on Providing Fast Money Transfer Services, Official Gazette No. 77/03) and the Law on Amending the Law on Providing Fast Money Transfer Services (Official Gazette No. 54/07, 48/10, 67/10, 17/11, 135/11, 187/13 and 154/15).

[19] Some sectors' specific indicators (e.g., for banks and life insurance companies) are further divided into indicators related to clients, products, transactions, etc.

The analysis of these documents shows that there are no specific indicators or case studies covering the scenarios related to online fraud and/or online money laundering that have been identified during the on-site mission. Nevertheless, some of the existing indicators can also assist obliged entities in preventing/detecting online fraud[20] and online money laundering. For this purpose, the indicators have been divided into those that apply to the suspect's account/transactions or to suspect's and victim's accounts/transactions.[21]

a) Indicators applying to the suspect's account/transactions:

- The client submits false or forged identification documents (Common indicators for all entities, Point 3).
- The client or third party originate from a state that does not comply with standards to prevent money laundering and financing terrorism (the list of FATF, EU, Council of Europe) or state known for producing, distributing or selling drugs or state known as a tax haven (Common indicators for all entities, Point 8).
- The client performs transactions in large amounts or performs transactions that do not correspond to his income (List of ML indicators for banks, Point 1.7).
- The client fails to submit the details for the person/s in whose name he acts (List of ML indicators for banks, Point 1.19).
- The client receives transfers on his account from persons who are not associated with the nature of his business activity (List of ML indicators for banks, Point 1.20).
- There is information that the client may be involved in illegal activities (List of ML indicators for banks, Point 1.22).
- The client origins from country, the bank considered as risky, and others (List of ML indicators for banks, Point 1.26).
- Successive money transfers, without any obvious purpose, or in order to cover up the trail of the money beneficiary (List of ML indicators for banks, Point 2.1).
- Transaction is based on consulting, intellectual, information or accounting services or services from the marketing field (List of ML indicators for banks, Point 2.5).
- Transaction performed by a non-resident natural person in amount of over 50.000 Euros in denar counter value or a non-resident legal entity in amount of over 100.000 Euros in denar counter value (List of ML indicators for banks, Point 2.8).
- Money transfers which the client immediately, in whole or approximately the same amount, transfers to third person (List of ML indicators for banks, Point 2.9).
- Large amounts of deposits are structured, accumulated, and further transferred to foreign bank accounts (List of ML indicators for banks, Point 2.11).
- Large transactions on accounts of recently established legal entities (List of ML indicators for banks, Point 2.12).

[20] CEO/BEC frauds in particular.
[21] No indicators were identified that would only apply to the victim's account/transactions.

- The client who receives large or frequent foreign inflows, failing to provide the necessary documents for the transactions' purpose and sends them to the sender i.e. transfers them to third parties (List of ML indicators for banks, Point 2.15).
- Frequent cash transactions, which are slightly below the legally established limit for reporting transactions to the Office (List of ML indicators for banks, Point 2.24).
- Frequent transactions based on advanced payment or return of advance for which the client gives explanation that is for unrealized business agreement (List of ML indicators for banks, Point 2.35).
- The client puts large amounts to an account and gives an order to the bank to transfer them to larger number of entities (legal or natural persons), especially when for such transaction there is no evident economic or visible legal purpose (List of ML indicators for banks, Point 2.37).
- The client performs high value transactions through bank payment card, using the advantage of the option for loading the card without physical presence in the bank (through ATMs, e-banking etc.) (List of ML indicators for banks, Point 3.8).
- Financial activities and transactions that do not comply with the client's age and occupation (List of ML indicators for the Post Office and the legal entities that perform telegraphic transmission or delivery of valuable shipments, Point 9).
- The client often receives money and immediately transfers them (List of ML indicators for fast money transfers and subagents, Point 8).
- Different clients send money to one and same person, and vice versa (List of ML indicators for fast money transfers and subagents, Point 10).
- The client's profile, i.e. his financial standing is not in proportion with the activity (List of ML indicators for fast money transfers and subagents, Point 11).
- The client often receives money whose total amount is significant (List of ML indicators for fast money transfers and subagents, Point 18).

b) Indicators applying to both victim's and suspect's accounts/transactions:

- Transaction with persons who originate from countries that the bank considered as risky (List of ML indicators for banks, Point 2.2).
- Changing the usual way, the client performs the transactions (List of ML indicators for banks, Point 2.3).
- Transaction from or to off shore country (List of ML indicators for banks, Point 2.4).
- Financial activities and transaction without economic justification (i.e. there is no economic nor some other kind of relation between the activity of both parties participating in the activity/transaction) (List of ML indicators for the Post Office and the legal entities that perform telegraphic transmission or delivery of valuable shipments, Point 10).

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, FIO and/or other

competent authorities may wish to consider improvements in the way in which online fraud and money laundering are prevented, detected and investigated. 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.

5.1 Legal/Policy Recommendations

This section provides legal and policy recommendations related to selected legal aspects of the obliged entities' AML/CFT obligations and FIO and other competent authorities' tasks and powers.

- The FIO 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 all competent authorities, including the competent law enforcement authorities, should be involved.
- The AML/CFT Law (Article 34, paragraph 1, fifth bullet point) should extend the reporting entities' obligation to adopt procedures for recognition of unusual transactions and suspicious transactions beyond money laundering and financing of terrorism (e.g., to cover all suspicious transactions with funds that are proceeds from crime).
- The authorities should consider extending the FIO powers to order a monitoring of a business relationship (Article 82 of the AML/CFT Law) and to order a temporary detention of a transaction and send a request for provisional measures to the competent public prosecutor (Article 83 of the AML/CFT Law) to cover also situations, where FIO suspects that an online fraud or other criminal offence (e.g., predicate offence for money laundering) has been committed, or attempted, with no suspicion of money laundering or terrorist financing whatsoever.
- FIO, 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 competent authorities may consider including in the list of indicators for suspicious transactions. In this regard, the FIO may use the existing structure of suspicious indicators or include an additional section with indicators that will only target the online fraud, other cybercrime offences and related money laundering.

<u>General indicators:</u>

- The transaction is related to the buying or selling of virtual currency (e.g., Bitcoins, LiteCoin, Ethereum, Zcash).

- The transaction is related to the 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/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 quotes as a legal basis for a transaction "*transfer", "gift", "consulting" or "business investment*".
- 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.
- Large incoming transactions on a previously dormant account or an account that was opened recently that cannot be properly explained or documented by the client.

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 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 differ.

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, 15-16 June 2017, Skopje, "The former Yugoslav Republic of Macedonia": https://rm.coe.int/3156-35-iproceeds-skopje-assessment-guidelines-for-private-sector-web/1680726eae
B. Cybercrime legislation - country profile – "The former Yugoslav Republic of Macedonia"
C. Law on Prevention of Money Laundering and Financing of Terrorism, Official Gazette, No. 130, dated 3 September 2014: http://www.ufr.gov.mk/files/docs/AML-CFT%20LAW%202014%20eng.pdf