iPROCEEDS

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

Version 9 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

Bosnia and Herzegovina

Project: iPROCEEDS

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1 Introduction

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

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

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

This report was prepared by Council of Europe experts, Dave O'Reilly (Ireland) and Klaudijo Stroligo (Slovenia) under the 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 Objective

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

[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.

1.2 Methodology

In preparing this report, the Council of Europe experts have conducted desk review of 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 held on 22-23 May 2017 in Sarajevo, Bosnia and Herzegovina, where they met with representatives of all relevant institutions.

1.2.1 Meetings

Meetings were held with the following agencies:

- Financial Intelligence Department, State Investigation and Protection Agency (SIPA), Ministry of Security (FIU);
- Cybercrime police of Brčko District;
- Cybercrime police from the Federation of Bosnia and Herzegovina;
- Police for financial investigations and money laundering investigations from Republika Srpska;
- Federal police for financial investigations;
- The Central Bank;
- The Banking Agency of the Federation of Bosnia and Herzegovina;
- The Banking Agency of Republika Srpska;
- The Insurance Agency of the Federation of Bosnia and Herzegovina;
- The Insurance Agency of Republika Srpska;
- The Association of Insurance Companies of the Federation and Republic Srpska; 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 and 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.

- 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 Financing of Terrorist Activities (AML/CFT Law)[3] and the Ordinance on the Implementation of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities (hereinafter referred to as Ordinance)[4] have been analysed and reviewed. In the assessment provided below, the most recent Council of Europe MONEYVAL Committee mutual evaluation report (MER)[5] on Bosnia and Herzegovina and other documents related to criminalisation of online fraud and other criminal offences mentioned in the Council of Europe Budapest Convention on Cybercrime have also been taken into account.[6]

2 Legislation

In Bosnia and Herzegovina, the Criminal Codes at entities' and Brčko District's levels prescribe criminal acts, including computer-related fraud and other offences related to cybercrime.[7] According to MONEYVAL 2015 MER on Bosnia and Herzegovina, the criminal act of money laundering is based on *"all crime"* approach[8] and is to a large extent criminalised in compliance with the relevant AML/CFT international standards.[9]

The reporting of suspicious transactions is regulated in Article 38 of the AML/CFT Law, which reads as follows:

"1) Obliged entity shall deliver to the FID the data referred to in Article 54 paragraph 1 relating to the following:

a) Any attempted or completed suspicious transaction, suspicious funds irrespective of transaction, suspicious client or person;

b) A cash transaction the value of which amounts to or exceeds BAM 30,000;

c) Connected cash-transactions the overall value of which amounts to or exceeds BAM 30,000.

2) When an obliged entity is to report about a suspicious transaction to the FID, they shall also inform on the following:

a) That a transaction by its characteristics relating to the status of a client or other characteristics of the client or funds or other characteristics evidently disagrees with usual transactions of same client, as well as that it corresponds to the necessary

[3] Law on the Prevention of Money Laundering and Financing of Terrorist Activities, Official Gazette of Bosnia and Herzegovina, No. 47/14 and 46/16.
[4] Ordinance on the Implementation of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities, Official Gazette of Bosnia and Herzegovina, No. 41/15.
[5] See MONEYVAL 2015 Report on Fourth Assessment Visit to Bosnia and Herzegovina (https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715b43).
[6] See the attached Council of Europe Cybercrime country profile of Bosnia and Herzegovina.
[7] Ibidem.
[8] This means that all criminal offences, including cybercrime related offences, are predicate offences for money laundering.
[9] See MONEYVAL MER on Bosnia and Herzegovina, pages 40 – 54.

number and types of indicators pointing to that there exist the reasons for a suspicion of money laundering or funding of terrorist activities;

b) That the transaction is directed to the avoidance of regulations governing the measures of the prevention of money laundering and terrorist activity financing."

In this regard, it is important to mention also a definition of "suspicious transaction" as provided in Article 3 of the AML/CFT Law.

"Suspicious transaction is a transaction for which obliged entity or a competent authority assesses that is related to the transaction or a person who is conducting the transaction, there are founded grounds for suspicion that criminal offences of money laundering or financing of terrorist activities have been committed, or that the transaction involves funds derived from illegal activities."

The analysis of these provisions shows that they are to a large extent compliant with the Financial Action Task Force (FATF) Recommendation 20[10] 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[11], which require reporting to the FIU any suspicion that the funds are the proceeds of criminal activity, or are related to terrorist financing. From the text above it can be seen that Paragraph 1, point a) of Article 38 and the definition of suspicious transaction in Article 3 are wide enough to cover all situations required by international AML/CFT standards. Even though Paragraph 2 of Article 38 seems to limit the reporting obligations only to cases covered by indicators for suspicious transactions related to money laundering and terrorist financing, the Ordinance issued by the Council of Ministers (see below) doesn't indicate the same.

The AML/CFT Law in Articles 47 and 53 further requires that the list of indicators for identification of suspicious transactions and clients is prepared by obliged entities in cooperation with the FIU and other supervisory bodies. In Article 85, the AML/CFT Law also authorises the Council of Ministers to adopt additional instructions/guidelines with regard to the application of relevant provisions of this law. Based on this provision, in 2015 the Council of Ministers issued the Ordinance that in Section III (Articles 12 to 26) includes guidelines for indicators of suspicious transactions, covering the general indicators as well as obliged entities' specific indicators.

It is clear from the above that the current legislative framework already requires the obliged entities to report to the FIU any suspicion of criminal activity or attempted criminal activity, including the online fraud and online money laundering. However, on the recipient's side the AML/CFT Law limits the powers of the FIU, so that they can only be used when there is a suspicion of money laundering or terrorist financing. This applies not only to the FIU powers to suspend suspicious transactions (Article 58) or

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

[11] 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).

order a continuous monitoring of financial businesses of a client (Article 60), but also to the FIU authority to request data from the obliged entities (Article 56) and to send their reports with the analysis to the competent prosecutor (Article 57).[12]

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.

3.1 Financial Intelligence Department

A meeting was held with representatives of Financial Intelligence Department placed in the State Investigation and Protection Agency (SIPA), Ministry of Security of Bosnia and Herzegovina (FIU).

The obligations of the reporting entities are described in the AML/CFT law, with a list of indicators being published in a separate ordinance. The indicators are adopted at the level of the Council of Ministers and the process for creation of the list of indicators is as follows:

- A group of advisers propose indicators for adoption.
- A draft ordinance is prepared by a working group:
  - The working group is headed by the Ministry of Security, with members from the FIU, Federal Ministry of Interior, Ministry of Security and Banking Agencies of the Federation and Republika Srpska.
  - Private sector entities are not represented at the working group, however the draft indicators were sent to them for comments.
- The Council of Ministers reviews and, in due course, adopts the ordinance.

[12] In practice, this means that if an attempted online fraud is reported by the bank to the FIU, the FIU is formally not allowed to send this information and its analysis to the competent law enforcement authority and/or prosecutor, because the AML/CFT Law requires the FIU to establish grounds for suspicion that money laundering or terrorist financing has been committed.

- The ordinance containing indicators is considered to be guidelines, which means that additional indicators can be developed and used if required.

The majority of the FIU's exposure to cybercrime related issues arises in the form of enquiries from foreign FIUs, principally relating to CEO/BEC fraud. However, several typologies were discussed:

Typology 1: (regarding payments from Germany to accounts in Bosnia and Herzegovina)

- Faxes were sent to issue instructions for transfers of between EUR 9,000 and EUR 10,000 from accounts in Germany to accounts in Bosnia and Herzegovina.
- Reports of the activity were received from both INTERPOL and from the banking sector.
- In total, orders for amounts totalling approximately EUR 1.5 million were directed to individuals in Bosnia and Herzegovina.
- Of the total EUR 1.5 million, approximately EUR 1 million was stopped and sent back to Germany.
- Of the EUR 500k transactions that were completed were paid into the accounts of individuals and later withdrawn in cash.
- The issue was mainly investigated by the federal police who identified one person who was suspected of organising the entire scheme.
- In 2016, the issue became an area of focus and in order to raise awareness a notice was circulated to banks with an indication that money was being sent to their accounts as part of a fraud scheme.
- Upon receipt of the awareness information, additional STRs were received.
- The investigation is continuing, including collection of evidence from Germany.

Typology 2: BEC/CEO fraud

- Emails were received by companies in Bosnia and Herzegovina purportedly from partner companies, usually located abroad, with whom the domestic companies had long standing relationships.
- Invoices were received with changed bank account details.
- Funds were thereby sent to accounts in Poland, UK and France in amounts ranging from EUR 20-30k (typical) to EUR 100k (maximum).
- The number of cases of this type has increased in recent years.
- Within Bosnia and Herzegovina, the competent authorities for investigation of fraud are at the entity level and the FIU has only been involved to assist with tracking the money.
- In all cases, the crime was detected by the victim(s) and not by the banks.

Several cases, representative of another typology, were also reported:

- Individuals, representing themselves as IT experts, communicate with natural and legal persons located in the foreign jurisdiction.
- They collect small amounts of money (EUR 100-200 is typical) by money remittance provider.
- The person in the foreign jurisdiction believes they are paying for the services of IT experts.
- Requests were received from the foreign FIU to check into the details of particular persons.
- Requests were sent to the relevant money remittance provider agency with Bosnia and Herzegovina for further information.

- It is not clear at the time of reporting whether this is a tax evasion matter or a fraud.

Some other case examples were also provided:

- Emails sent by unknown persons to foreign individuals with a story of hardship and asking for funds to be transferred.
- Emails sent by unknown persons offering ways to earn large amounts of money, requesting a payment in advance.
- Emails sent by unknown persons containing work advertisements offering work in other countries in the EU, requesting a payment in advance.

A hypothetical scenario was presented as follows:

- A financial institution uses a fraud prevention measure to detect changes to the IBAN (bank account details) of existing client relationships.
- When such cases arise, fraud may be prevented because the client can be contacted and asked to confirm the changed details.
- Therefore, there is no money laundering and only attempted (but prevented) fraud.
- International standards require that obliged entities report suspicion of both attempted and successful money laundering and associated predicate offences.

The FIU explained that it would be unlikely that the banks would report such attempted but unsuccessful predicate offences to the FIU.

Finally, it was reported that the national money laundering risk assessment conducted in Bosnia and Herzegovina identified cybercrime, and CEO/BEC fraud typology in particular, as requiring attention.

3.2 Cybercrime Police

A meeting was held with representatives of several police forces:

- Cybercrime police of Brčko District;
- Cybercrime police from the Federation of Bosnia and Herzegovina;
- Police for financial investigations and money laundering investigations from Republika Srpska; and
- Federal police for financial investigations.

The first request was for the police agencies to elaborate on the two typologies provided in the FIU meeting (described above), and it was reported as follows:

Typology 1: (regarding payments from Germany to accounts in Bosnia and Herzegovina)

- In this case companies in Germany had been hacked and invoices had been altered.

Typology 2: BEC/CEO fraud

- A considerable number of incidents of this type have taken place in the last five years.
- The injured parties are legal persons.
- The amounts involved (the amount of damage) varies from between approximately EUR 5,000 to EUR 75,000.
- Most of the incidents are based on email correspondence.
- Mails are sent purportedly from partner/client companies in one of the following ways:
  - An unidentified person would intercept the correspondence between the companies in an unknown way, one company is in Bosnia and Herzegovina and one person is abroad. The unidentified person waited for the company from abroad to send a pro-forma invoice to the company in Bosnia and Herzegovina. The unidentified person alters the invoice and changes the payment details.
  - A domain is registered that looks very similar to the domain of the partner/client. Emails are then sent to the victim company that look superficially similar to emails from the legitimate source.
- The unidentified person alters the invoice and changes the payment details.
- In 95% of cases the altered bank account is in the UK.
- In many cases staff in the victim companies process the payments.
- In a number of cases the staff in the victim noted the changed details and when they queried the change (with the attacker by email), they were told that the partner/client had changed banking arrangements due to high fees at their previous bank.
- Requests for payment typically are received late on a Friday afternoon.
- The attacker(s) exploit time zone differences by making withdrawals several hours after domestic banks have closed.
- At least six of these incidents have been reported.
- Through Interpol some limited information was received about the beneficiaries to which the payments were made.
- Usually when requests are made, it is necessary to file an international legal assistance request.
- Analysis of the emails involved suggests that emails were sent using online platforms that were free of charge.
- In some cases where it was possible to identify the holder of the destination bank account, it was noted upon investigation that the accounts were opened with fake documents.

No instances of the communication between the bank and their client being hacked have been reported.

Another recent typology was presented, as follows:

- A company received an email with the subject "Indirect taxation authority of the Federation of Bosnia and Herzegovina".
- The employee that received the email thought that the tax authority had send a request/notification so they opened the email attachment.
- The attachment contained a malware that was installed on the employee's computer.
- Through the malware an attacker connected remotely to the employee's PC and made several large transactions to domestic bank accounts.
- The bank accounts had been opened recently and apparently specifically for this purpose.

- All of the transfers happened on a Friday.
- The individuals that were identified were those that withdrew cash from the domestic accounts, but they were just acting as mules, handing over the cash to someone they did not know.

The delegates highlighted a challenge with such cases where it is very difficult through police channels to get details about owners and activity of foreign bank accounts, with all responses indicating that formal mutual legal assistance requests are required. The delegates indicated that they have in the past used FIU powers to block accounts and get information on the holders of accounts.

It was acknowledged by the delegates that more could be done to raise awareness and share information to enhance preventative action. One example of an information sharing initiative was provided whereby meetings take place with the private sector in Brčko District to exchange information. It was observed by one delegate that information tends to circulate much more quickly between private sector entities (e.g. banks) than between police forces. The financial institutions have a forum where they meet periodically to exchange information and discuss fraud problems in general.

The representatives from the Federation of Bosnia and Herzegovina reported that they received requests from INTERPOL regarding cybercrime and Internet fraud. The requests were mostly related to the identification of the user of IP addresses located in Bosnia and Herzegovina. One specific case was described as follows:

- A person who was from Bosnia and Herzegovina but also a citizen of Germany together with his associates set up a network of mules all across Bosnia and Herzegovina.
- The mules received money in amounts slightly below the obliged reporting limit from natural and legal persons in Germany.
- The mules withdrew the money and kept around 1% of the funds.

An example of another specific case was described as follows:

- An individual working as an IT expert/engineer.
- He was engaged legitimately on contract to provide IT maintenance service to a company.
- The company noticed that a small amount of money had been taken from their account.
- Through investigation it was identified that the IT expert/engineer was the culprit, although he was somewhat difficult to identify because he was not an employee but rather contracted to provide IT support.
- The funds were transferred to a sports betting shop.
- He also used credit cards of others to purchase equipment (computers, mobile phones, etc.)

Yet another example of a specific case was described as follows:

- Compromised bank account information was used to transfer money (amounts in the region of EUR 1,000 to EUR 1,500) to online gambling accounts.
- The online gambling account holder was playing poker and lost all of the funds.
- In due course, the person was arrested and revealed that the funds that had been lost were in fact lost to a second online gambling account that he also controlled. Initially he used the same IP address to register both players, and later changed the IP address, because playing on both sides via the same IP address was prohibited.

The details of operation of various ransomware attacks that have been reported were also described as follows:

- Approximately once a month a ransomware incident is reported.
- Sometimes people pay and get the data back; others pay and get some or none of the data back.
- A final group pay, get the data back but then it is re-encrypted again.
- Payments are typically in Bitcoin but a lot of victims don't know how to pay in Bitcoin.
- Sometimes payments are made by bank transfer or Western Union.

In addition, several examples of misuse of credit cards were provided:

- Example 1
  - Compromised credit card details are used to purchase train tickets.
  - The train tickets are later cancelled.
  - Through the specific online booking platform concerned, it is possible to refund to the same bank account/credit card or a different one.
  - There have been cases where the money is refunded to a different bank account.

- Example 2
  - Compromised credit card details used to purchase plane tickets online in foreign jurisdictions.

3.3 Central Bank and Banking Agencies

A meeting was held with representatives of the Central Bank, the Banking Agency of the Federation of Bosnia and Herzegovina and the Banking Agency of Republika Srpska.

The delegates reported that a handful of BEC/CEO fraud and the use of money mules have been identified and advisories have been circulated to all financial institutions.
Moreover, recently a number of problems have been experienced with transactions originating on the PayPal platform. The root of the problem is that insufficient details of the sender of the funds and purpose of transaction are provided on the incoming transfer and is it not possible to ascertain whether the funds have a legitimate source.

In Bosnia and Herzegovina, virtual currencies are not regulated in any way (either forbidden or allowed).

There are a small number of cases of abuse of electronic banking systems. The cases reported involved the opening by third parties of bank accounts in various banks and then the transfer of funds from victim accounts into the accounts of these third parties. All such cases are reported to the FIU.

In most cases the financial institutions have software systems that support the indicators.

3.4 Securities Commissions

A meeting was held with representatives of the Securities Commissions of Brčko District, Republika Srpska and the Federation of Bosnia and Herzegovina.

The delegates were not aware of any typologies in their sector involving online crime, insider trading or market manipulation involving cybercrime. It was indicated that in cases of fraud successfully prevented by an obliged entity, it is expected the incident would be reported to the FIU.

In Bosnia and Herzegovina, trading in virtual currencies (Bitcoin in particular) is not acceptable and such trading is not allowed.

The expectation is that brokerage that is part of a bank will be well-equipped to detect indicators for fraud and money laundering. A screening of reporting entities was carried out and it was found out that some are better equipped than others, with small single person brokerages being unlikely to have any capabilities in place to detect indicators of fraud and money laundering. The screening process is at the stage where the report is close to finalisation and recommendations are to be made. Similar situations were reported by all securities commissions in their respective areas.

The obliged entities tend to report anything, even if they are not sure whether they are obliged to report. One delegate recalled an instance where a client was reluctant to provide all required documentation and in this case the broker reported his suspicion to the FIU.

During the recent national ML/TF risk assessment the securities issued by the entities or the state (debt securities, treasury bills, bonds) were assessed as low risk for ML/TF, with other securities (stocks) being assessed as medium to high risk. However, there is very little data available upon which to base the assessment of the securities market due to the shallowness and low liquidity of the markets.

3.5 Insurance Supervision Agencies and Associations of Insurance Companies

A meeting was held with representatives of the Insurance Agency of the Federation of Bosnia and Herzegovina, the Insurance Agency of Republika Srpska and the Association of Insurance Companies of the Federation and Republic Srpska.

The representatives indicated that virtually all communication between insurance agencies and their clients in life insurance is face-to-face.

The delegates were only aware of one cybercrime related case, where a malware was sent to an insurance company that blocked access to their computers. An amount of 1.000 USD was requested to be paid via PayPal for unblocking their IT system. They managed to unblock their computers and the cases was not reported to the police. No other fraud or online crime proceeds typologies were detected in their sector.

During their national ML/TF risk assessment, the examined life insurance products were assessed as low risk. This is because products with investment features don't exist in this sector and are not used in Bosnia and Herzegovina. Moreover, the liquidity in life insurance market is very low and average premium is around 250 EUR.

3.6 Banks and Banking Association

A meeting was held with representatives of several banks and the Banking Association.

In banks, the AML/CFT and fraud functions are usually covered by one of the following departments:

- Compliance department
- Operational risk department
- Legal department

In cases of fraud (e.g., CEO/BEC cases), where there are losses either to the bank or to the customer, the bank would make a formal complaint to the police. The FIU is now willing to accept these cases so the banks report to the FIU as well as to the police (especially in money mule cases).

In Bosnia and Herzegovina, the CEO/BEC fraud and various types of card fraud (skimming, online, counterfeit cards) were the most common typologies.

With regard to indicators of commonly experience cyber-fraud types, the delegates provided the following suggestions:

- CEO/BEC fraud can sometimes be detected due to language errors in the email (e.g., perpetrators are using the Google translate).

- CEO/BEC fraud can sometimes be prevented by implementation of either technical or manual controls to detect when payment instructions for established customer relationships change.
- Money mule activity has been noted to involve a significant number of transactions originating in German speaking countries.
- Money mule activity has been noted to involve transactions in the amounts of EUR 9,000 to EUR 10,000 (close to the reporting limit).

Some successes have been achieved in cases involving money mules by contacting the sender to confirm the transaction. In some cases, the sender has reported the transaction as fraudulent, which has led to the recipient account being closed and reported to the FIU.
Other indicators used frequently by the financial institutions were:

- Owners of companies making loans to the company; and
- Dividends being paid by companies as a component of a money laundering scheme.

The delegates reported that transactions involving virtual currencies are usually blocked. It was suggested that the use of virtual currencies could be used as an indicator of fraud and/or money laundering, although this indicator alone is not definitive.

4 Indicators

As mentioned above, the indicators for suspicious transactions are provided in Section III of the Ordinance. The analysis of these indicators shows that there are no cybercrime specific indicators included in the list of indicators and 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 general indicators and indicators related to the banking sector have been identified that can also assist obliged entities in preventing/detecting online frauds[13] and online money laundering. These indicators can be divided into those that apply to the victim's account and those that are relevant for the suspect's/fraudster's account or to both.

a) <u>Indicators applying to the victim's account:</u>

- The client transfers large sums of money abroad with instructions to a foreign person abroad to make payments in cash (Article 18, point (a) of the Ordinance).

[13] CEO/BEC frauds in particular.

b) Indicators applying to the suspect's account:

- The client starts carrying out frequent cash transaction of large amounts, which was not a normal activity of that client in the past (Article 12, point (e) of the Ordinance).
- The client constantly carries out cash transactions which are slightly below the threshold amount for which there is an obligation of identifying i.e. reporting (Article 12, point (g) of the Ordinance).
- The client carries out a transaction in an amount that is unusual compared to amounts of past transactions (Article 12, point (h) of the Ordinance).
- Transaction which results in significant, but inexplicable, activity on the account which was previously mostly dormant (Article 12, point (m) of the Ordinance).
- Transaction that do not correspond to the knowledge and experience of the obliged entity about the client and the declared purpose of business relationship (Article 12, point (n) of the Ordinance).
- The client was prosecuted for a criminal offence (Article 12, point (bb) of the Ordinance).
- The activity in the account by far exceeds the activity which was foreseen at the time of account opening (Article 13, point (f) of the Ordinance).
- Dormant account that suddenly starts to be used actively (Article 13, point (g) of the Ordinance).
- The client has never been employed and has significant funds in the account (Article 16, point (j) of the Ordinance).
- The client consistently withdraws large sums of money from the account into which a large and unexpected amount of funds from abroad has just been remitted (Article 17, point (e) of the Ordinance).

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

- The transaction involves a country or territory in which there is no effective system of prevention and detection of ML/TF (Article 14, point (d) of the Ordinance).
- The transaction involves a country which is known, or suspected, to assist ML activities or of supporting TF (Article 14, point (f) of the Ordinance).

5 Recommendations

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

5.1 Legal/Policy Recommendations

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

- The reference to indicators in Paragraph 2, Point (a) of Article 38 of the AML/CFT Law should be amended so that in addition to suspicion of money laundering and terrorist financing the text includes also a suspicion of other criminal offences (e.g. a suspicion that funds are the proceeds of any criminal activity).

- The FIU powers to suspend a suspicious transaction (Article 58), to order a continuous monitoring of financial businesses of a client (Article 60), to request data from the obliged entities (Article 56), and to send their reports with the analysis to the competent prosecutor (Article 57) should be extended to cover also situations, when the FIU suspects that an online fraud or another criminal offence has been committed, or attempted, with no suspicion of money laundering or terrorist financing whatsoever.

- The banks and other obliged entities should be instructed to report their suspicion of CEO/BEC frauds or attempted frauds simultaneously to the FIU and the competent police authority/prosecutor to ensure that these authorities can promptly take all the necessary measures within the scope of their powers.

5.2 Indicators

This section presents examples of additional indicators for prevention and detection of online frauds and money laundering that the FIU and/or other competent authorities may wish to consider including in the list of indicators for suspicious transactions. In this regard, the authorities may use the existing structure of the guidelines for indicators for suspicious transactions in the Ordinance (e.g. division per sector/businesses/product)[14] 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 buying or selling the virtual currency (e.g., Bitcoins, Litecoin, Ethereum, Zcash).
- The transaction is related to transfer of winnings from an online gambling platform.
- The client requests a transaction to be carried out urgently or that it should be treated as confidential.

<u>Indicators related to bank accounts:</u>

- The client receives a payment via PayPal that does not include details of the sender or purpose of the transaction.

[14] As presented below.

- 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 close 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.
- 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.
- Instructions for payment are received from a new employee of the corporate client.

Indicators related to territories outside Bosnia and Herzegovina:

- 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).

6 Appendixes:

A. Agenda of the assessment mission of guidelines to prevent and detect/identify online crime proceeds, 22-23 May 2017, Sarajevo, Bosnia and Herzegovina: https://rm.coe.int/3156-35-iproceeds-assessment-guidelines-for-private-sector-bih/1680715c24
B. Cybercrime country profile – Bosnia and Herzegovina (version of 30 January 2017).