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

Kosovo*[1]

Project: iPROCEEDS

www.coe.int/cybercrime

[1] *This designation is without prejudice to position on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

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.[2] Often the chain is "broken" by cash operations performed traditionally 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, 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 recognize the suspicious patterns related to their clients, products, services and transactions.

In this regard, international AML/CFT standards[3] 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.

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

1.1 Objectives

The main objective of the report is to put forward a set of recommendations for elaboration and/or improvement of guidelines and indicators for financial sector entities to prevent and detect online fraud and money laundering in the online environment. The report is also aiming to address some legal and policy issues identified during the project cycle that could hamper the effective use of these guidelines and indicators in practice.

[2] 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).
[3] See FATF Recommendation 34.

1.2 Methodology

In preparing this report, the Council of Europe experts have conducted a 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 Pristina, Kosovo* on 19 – 20 June 2017, where they met with representatives of several institutions and state bodies.

1.2.1 Meetings

Meetings were held with the following agencies:

- Financial Intelligence Unit (FIU-K);
- Cybercrime Unit, Kosovo* Police;
- Integrated Financial Investigation Unit, Kosovo* Police;
- The Central Bank; 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:

- 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 the Prevention of Money Laundering and Combating Terrorist Financing (AML/CFT Law)[4], the FIU-K List of Indicators for prevention of money laundering[5], the FIU-K List of Indicators for prevention of terrorist financing[6], the FIU-K Typologies of money laundering and terrorist financing in the Republic of Kosovo*[7], and the Criminal Code[8] have been analysed and reviewed. In the assessment provided below, some other documents related to criminalization of online fraud and other criminal offences mentioned in the Budapest Convention on Cybercrime have also been taken into account.[9]

2 Legislation

In Kosovo*, all criminal offences envisaged under the Budapest Convention on Cybercrime,[10] including the computer-related fraud[11], are covered and are included in the Criminal Code and in the Law on Prevention and Fight of the Cybercrime.[12] The criminal act of money laundering (Article 308 of the Criminal Code and Article 56 of the AML/CFT Law) is based on *"all crime"* approach[13] and is 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 26 of the AML/CFT Law, which reads as follows:

"All reporting entities shall report to the FIU-K, in the manner and format specified by the FIU-K all suspicious activities or transactions within twenty-four (24) hours from the time the activity or transaction was identified as suspicious; and …)."

In this regard, it is important to mention also a definition of term "suspicious act or transaction" as provided in Article 2 of the AML/CFT Law.

"Suspicious act or transaction - an act or transaction, or an attempted act or transaction, that generates a reasonable suspicion that the property involved in the act or transaction, or the attempted act or transaction, is proceeds of crime or is related to terrorist financing and shall be interpreted in line with any sub-legal act issued by the FIU-K on suspicious acts or transactions."

The analysis of these provisions shows that the obligation to report suspicious transactions covers not just cases of money laundering and terrorist financing but also cases related to activities or transactions with funds that are proceeds of any criminal activity. It can be therefore concluded that these provisions are fully compliant with

[4] See Appendix C.
[5] See Appendix D.
[6] See Appendix E.
[7] See Appendix F.
[8] See Appendix G.
[9] See the Council of Europe Cybercrime legislation - country profile, Kosovo* (Appendix B).
[10] Kosovo* is not a Party to the Budapest Convention on Cybercrime.
[11] In Kosovo*, the computer-related fraud is included in Article 16 of the Law on Prevention and Fight of the Cybercrime under the title "Causing loss of asset".
[12] Ibidem.
[13] This means that all criminal offences, including cybercrime related offences, are predicate offences for money laundering.

the Financial Action Task Force (FATF) Recommendation 20[14] and Article 33 of the EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[15], which both require obliged entities to report to the FIU 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 Paragraph 1, Point 1.11.2 of Article 14 further requires that the list of indicators of suspicious acts or transactions is prepared by the FIU-K. Based on this provision, the FIU-K drafted the list of indicators for both prevention of money laundering and terrorist financing. While the list of money laundering indicators includes several general indicators and some obliged entities' specific indicators related to this topic, it remains unclear why it was not extended to cover also other relevant criminal activities (e.g., those related to predicate offences for money laundering).

Furthermore, the AML/CFT Law in Paragraph 2, Point 7 of Article 17 also authorizes the obliged entities to *"supplement the FIU-K list of indicators with specific indicators for a reporting subject to identify persons and transactions with respect to which there is reason to suspect money laundering or terrorist financing."* It is not known if in practice such indicators have indeed been developed by obliged entities and, if yes, in which sectors.

It is clear from the above that the legislative framework requires the obliged entities to report to FIU-K 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 FIU-K as well as Article 17, Paragraph 2, Point 7 of the AML/CFT Law are somehow limiting the scope of reporting only to money laundering and terrorist financing.

On the recipient's (FIU-K) side the AML/CFT Law is not entirely clear about the powers of FIU-K and whether they can only be used for the purpose of detecting and preventing ML and TF or also for detecting and preventing predicate offences. While some provisions of the AML/CFT that regulate the FIU-K powers only refer to ML/TF, others also include a reference to predicate offences. For example, it seems that the following provisions of the AML/CFT Law only apply to ML and TF:

- Article 4 of the AML/CFT Law which is defining the FIU-K functions;
- Article 27 which regulates the FIU-K power to temporary freeze a transaction; and
- Article 39, Paragraph 5 which requires FIU-K to provide feedback to obliged entities on reported suspicious transactions.

[14] See the FATF 2012 Forty Recommendations (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html).
[15] See the Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849).

On the other hand, Article 14, which regulates duties and competences of FIU-K, links these duties also to predicate offences for money laundering. For example, these apply to FIU-K power to:

- Receive voluntarily provided reports and information (Paragraph 1, Point 1.1.3);
- Collect information from publicly available sources (Paragraph 1, Point 1.2);
- Conduct strategic analysis (Paragraph 1, Point 1.3); and
- Disseminate the outcome of its analysis to the relevant authorities.

In practice, this means that if, for example, a transaction related to an attempted online fraud is reported by the bank to FIU-K, the latter is formally not allowed to freeze such transaction; however, it may send this information and its analysis to the competent law enforcement authority and/or prosecutor. During a desk review, the objectives behind the explained division related to the use of FIU-K powers remain unclear.

3 Typologies and Selected Case Studies

As mentioned in Section 1.2.1, meetings were held with various agencies to understand:[16]

- 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.

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

3.1 Financial Intelligence Unit of the Republic of Kosovo* - FIU-K (Ministry of Finance)

The FIU-K publishes a very broad list of indicators for recognising suspicious transactions, including ones for banks and other reporting entities (lawyers, notaries, accountants, auditors, etc.). The published indicators do not contain any cybercrime or online money laundering specific indicators. It was reported that the published lists are revised periodically and interim bulletins are also published, meaning that the opportunity exists to publish cybercrime specific indicators if appropriate.

It was recognised by the FIU-K that there is a need for cybercrime specific indicators and that reporting entities are missing indicators regarding cybercrime. It was further reported that banks have, in fact, asked for such indicators to fight cybercrime.

[16] The link to the outline of the meetings is enclosed – see Appendix A.

There have been a small number of suspicious transactions reported with elements of cybercrime and it was speculated that this may be due to lack of knowledge or lack of indicators on the part of the reporting entities.

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 to the FIU any suspicion that funds are the proceeds of a criminal activity, or are related to terrorist financing.

Such cases would report by the banks to the Cybercrime Unit in the police and it would be unlikely that the banks would also report to the FIU-K. It was further indicated that whether such an incident would be reported to the FIU-K would depend on what phase of money laundering was involved. For example, if money had transited through multiple accounts (i.e., the money had been moved from the account into which the victim funds were originally transferred) then this would be reported to the FIU-K.

The AML/CFT Law defines the connected cash transactions as those happening within 24 hours. In some countries, the period for connected transactions is longer (ranging sometimes up to 5 - 7 days) and FIU-K indicated that their published indicators suggest that longer periods for connected cash transactions can be considered. Additionally, structured withdrawal of funds in amounts below reporting limits (regardless of time limit) is, separately, also in the published indicators. The FIU-K also explained that in practice only financial institutions and microcredit institutions support these indicators by sophisticated software systems, while other, smaller institutions, such as money exchange agencies, are family-run businesses and they are lacking resources to buy such software.

The FIU-K reports and analyses are circulated to several departments within the law enforcement agencies, depending on the typology of the crime. Some examples were provided as follows:

- If a suspicion of money laundering is detected, the FIU-K will report to the special prosecutor's office, the police and the tax administration. Very complicated or delicate cases are sent directly to the special prosecutor's office.
- If there is a suspicion of a tax avoidance but not money laundering, this is reported to the tax administration and also to the police, if there is a criminal offence. Typically, both institutions will be notified to facilitate cooperation if appropriate.
- If there is an online fraud with no elements of money laundering, this will be reported to the Cybercrime Unit.

Cooperation with law enforcement is possible within current legislation and FIU-K receives approximately 3-4 requests every year from the cybercrime police. In most cases, these requests are related to the misuse of credit cards, with some cases

involving PayPal to withdraw or launder money, and the FIU-K usually collects and provides the requested data.

A counter-example was also provided whereby there was a request from a court to identify all accounts of a person, but the case did not involve an element of money laundering, rather it was a case of non-payment of tax. Therefore, the FIU-K did not assist in this case.

All suspicious transaction reports (STRs) and cash transaction reports (CTRs) from obliged entities are received electronically, either directly in XML format or in the form of an excel spreadsheet which is filled out by the obliged entity and submitted. The FIU-K requires that in the STRs the obliged entities specify which indicator from the published list of indicators has triggered a report but they can also specify "other" and explain their suspicion.

In 2016, the FIU-K received 485 STRs with approximately 5-8 being related to cybercrime, online fraud or other online criminal activity. Several cases involving PayPal have been reported, as follows:

Typology 1: Advance Fee Fraud

- Goods or services were being offered online.
- Prospective customers pay a deposit and then the goods or services are never delivered.
- Payments are made either using credit cards or PayPal.
- A similar typology has been observed with insurance for work-related risk.

Typology 2

- Several cases of terrorist financing through the purchase of airplane tickets paid via PayPal.

The root of the problem is that financial institutions accept incoming transactions from PayPal but the transactions do not contain sufficient information about the payee or the purpose of the transfer.

Additional examples of the laundering typologies involving PayPal were provided as follows:

- Verified PayPal accounts being compromised and funds either stolen or transited to these accounts.
- Individuals using PayPal accounts to purchase fictitious goods from themselves where the goods do not exist.

Regarding the virtual currencies, at present they are not regulated Kosovo*. According to the FIU-K the trend is to purchase virtual currencies through websites using credit cards and then sell them on the black market. However, the purchase and sale does not take place through any institution in Kosovo* because there is a lack of regulation.

FIU-K has not received any STRs related to CEO/BEC fraud. Several other typologies were provided by the FIU:

Typology 1

- Individuals apply for credit cards in foreign jurisdictions (Gibraltar was highlighted in particular).
- The plastic cards are then sent to Kosovo* and used to withdraw funds from ATMs.
- The banks in Kosovo* cannot detect and report who is withdrawing the money because there is insufficient information available to them to do so.
- At present the limit for ATM withdrawal is EUR 2,000 in 24 hours.
- This means that in 10 days an individual can withdraw EUR 20,000 in cash and this is impossible to detect and prevent within Kosovo*.

Typology 2

- Bank transfers to accounts in Cyprus, which are later identified as being the accounts of virtual currency exchanges.
- Investigations are on-going but it has not yet been possible to establish whether the virtual currency exchanges are established in the UK or Cyprus.

3.2 Cybercrime Unit and the Financial Investigation Unit in the Kosovo* Police

A hypothetical scenario was presented whereby a bank detects and prevents fraud (e.g., CEO/BEC fraud) and the question was asked whether, and to whom, such an incident might be reported. It was indicated that typically the bank would ask the client to report to the police. Usually the client will go to their closest police station to report the crime. The case will be assessed to determine whether the local police will investigate or engage the cybercrime unit to assist. In some cases, the cybercrime unit advises the local police but in the scenario presented the case would typically be transferred to the cybercrime unit. In summary, the reports mostly come from the victims but in certain cases the banks will directly report the crime to the police.

During the meeting, the following examples about recent experience with fraud or cybercrimes linked with financial transactions were provided:

Typology 1: BEC/CEO fraud

- An increasing number of such cases are being experienced.
- Fake emails are sent to a bank client, typically purporting to originate from businesses abroad, addressing businesses in Kosovo*.
- The language of these emails (whether received in English or Albanian) is usually improper.
- In 2015, more than 2 million EUR of losses were caused to companies in Kosovo* by this typology.

Typology 2: Malware-as-a-service

- Individuals producing and selling malware.
- Payments are made in Bitcoins.

Typology 3: Ransomware

- Ransomware was used to encrypt either individual or business data.
- Ransom was paid in Bitcoins (1 or 2 Bitcoins was typical, but up to 4 Bitcoins was also observed).

Typology 4: Forex fraud

- Stolen/cloned credit cards are used to buy goods (typically for computers or iPhones) online from companies in Kosovo* and shipped to addresses in Germany.
- Smaller amounts of money are involved.

There have been no reports of CEO/BEC fraud experienced in relation to other financial instruments (such as bonds, etc. targeting capital markets brokers). Moreover, participants did not recall receiving any reports from remittance providers. In several cases the police have approached money remittance providers directly in relation to on-going cases and in these cases the money remittance providers gave information about which country the money was transferred to.

Regarding virtual currencies, it was confirmed that they are not regulated or prohibited in Kosovo*.

The use of incoming PayPal transactions was also highlighted as presenting an investigative challenge, the reason being that the incoming transaction only says "PayPal" without any other information about the sender of the funds.

The Criminal Procedure Code regulates parallel financial investigations and while this can also be applied in cybercrime investigations, in practice it has only been conducted in couple of cases. The financial investigation can only be ordered by a prosecutor and during such investigation, intelligence can be requested directly from the FIU-K (without a prosecutor/court order). If the information is useful, a prosecutor/court request can be made to collect the information in an official way.

The AML/CFT Law allows the information provided by the FIU-K to be used as evidence on the approval of the director of the FIU-K. It was reported that this provision is only used in exceptional cases such as cases related to terrorism.

3.3 Central Bank

A meeting was held with representatives of the AML/CFT division of the Central Bank (CB). This division was established in 2013, with responsibility for both on-site and off-site examination of compliance with the AML/CFT legislation.

It was reported that while some of the banks have a separate, independent, AML/CFT unit, in others the AML/CFT function is part of the general compliance department. CB has recently published a new regulation that requires banks to have both a compliance officer and also an AML/CFT compliance officer, with both of these functions having to be at senior management level and both roles cannot be filled by the same person.

The legislation also requires that financial institutions need to do a money laundering and terrorist financing (ML/TF) risk assessment for each client based on products, transactional channels, and services used. However, the current high-risk categorization only includes the politically exposed persons (PEPs), NGOs, correspondent banking, non-compliant countries' risk and UNSC/EU sanctions related risk. In practice, the banks are using additional risk-categorisation modules but these are not specified in legislation.

The biggest banks[17] in Kosovo* are all supporting their clients' ML/TF risk categorisation and indicators for recognizing suspicious transactions with a sophisticated software. Currently, two of the banks are still using a manual process, but have already started to develop the necessary software. The same situation is in the micro-finance institutions[18] and remittance providers[19]; all big players have already in place the software to detect suspicious transactions.

Regarding the cybercrime typology, the CB is aware of cases where the bank clients' communication with their business partners has been compromised and incorrect payment instructions have been provided to banks by their clients (CEO/BEC fraud). In cases where the banks did not refund the defrauded funds, the victims complained to the CB. The delegates did not know whether the proposed changes to existing customer relationships (e.g., change of IBAN code of established customer relationship) would be actually detected by financial institutions.

Mobile banking is widely available and commonly used in Kosovo* and online banking is also being used increasingly.

Virtual currencies are not regulated in Kosovo*, however a public awareness message has been published warning about the risks associated to the use of virtual currencies. PayPal is also not regulated in Kosovo*.

There is generally good recognition within banks of their AML/CFT obligations and the banks are quite well prepared to generate appropriate STRs. There is generally a low ML/TF risk appetite within banks and risky customers are not easily accepted or are (at least) escalated to management before accounts are eventually opened. The AML/CFT awareness within the insurance sector is, however, on a considerably lower level.

[17] At the time of the visit, there were 9 banks registered in Kosovo* that were mostly owned by German, Austrian, and Slovenian banks.
[18] At the time of the visit, there were 20 micro-finance institutions registered in Kosovo*.
[19] In the remittance sector, the most important players are Western Union, MoneyGram and RIA.

3.4 Banks and the Banking Association

A meeting was held with representatives of several banks and the Banking Association (BA). In the BA, they have established several committees, including the Anti-Fraud Committee, the AML/CFT Committee, and the IT Security Committee.

The definition in legislation of suspicious transactions/activities is very broad, and a practice has been built to report cases of credit card fraud or other type of fraud (particularly the prevented fraud) only to the police. The banks believe that reporting such cases to the FIU-K and then to the police is a somewhat indirect route to report such cases. It was further explained that the banks have good relationships with the relevant police units.

The banks are detecting a lot of incoming PayPal transactions and for them it is difficult to establish if these transactions represent legal or illegal business. In these cases, they report such transactions to the FIU-K. Similarly, they report to the FIU-K cases where suspicious card payments or online payments have been made. While the CB has been working on a statement regarding PayPal, Visa and MasterCard require working with PayPal.

Most banks use the Siron software to support ML/TF indicators.

A hypothetical scenario of CEO/BEC fraud was presented and the participants agreed that a change of IBAN code for established customer relationships would be a useful new indicator in such cases.

Regarding the potential high-risk clients from off-shore jurisdictions, the banks explained that there are not many such clients in Kosovo*, because in order to open a non-resident account in a bank a foreign company has to register its business in Kosovo*. This significantly reduces the banks' ML/TF risk exposure.

The use of e-commerce to purchase goods is not common within Kosovo*. E-commerce transactions mostly involve money sent to recipients in Kosovo* who are usually young people providing services to foreign companies. Otherwise, it is much more common for PayPal to be used to send/receive money.

Finally, on the topic of virtual currencies it was reported that as an internal policy matter several financial institutions disallow the use of virtual currencies.

4 Indicators

As mentioned above, the indicators for suspicious transactions related to money laundering were drafted by FIU-K and published on their website[20]. In the introductory part of this section the objectives and scope of indicators are described as follows:

[20] See Appendix D.

"*The indicators of potential money laundering are primarily intended to raise awareness among reporting subjects in accordance with LPMLTF. The indicators are not intended to be exhaustive and provide examples only of the most basic ways by which money laundering may happen*."

The indicators are divided into the following two categories: i) General indicators and ii) Specific indicators[21]. Moreover, in 2013 – 2014 the FIU-K also published a document called "*Typologies of money laundering and terrorist financing*"[22], which contains several case studies related to different sectors, products, services and transaction channels as well as to different predicate offences.

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 expert mission. Nevertheless, some of the existing indicators have been identified that can also assist obliged entities in preventing/detecting online fraud[23] and online money laundering. For this purpose, the indicators have been 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/transactions:</u>

- Beneficiary account is not properly identified (List of ML indicators, General indicators, Point 1.8).

b) <u>Indicators applying to the suspect's account/transactions:</u>

- A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is carried out to, through or from locations of specific concern (List of ML indicators, General indicators, Point 1.1).
- A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed (List of ML indicators, General indicators, Point 1.2).
- Account activity inconsistent with customer profile (List of ML indicators, General indicators, Point 1.3).
- An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity (List of ML indicators, General indicators, Point 1.7).
- Cash withdrawals conducted at various bank branches and/or ATMs on the same day (List of ML indicators, General indicators, Point 1.9).
- Multiple low-value funds transfers which appear to be linked (List of ML indicators, General indicators, Point 1.28).
- Multiple low-value international funds transfers which appear to be linked, possibly indicating a large amount of funds broken down into smaller amounts (List of ML indicators, General indicators, Point 1.29).
- Similar transactions conducted over a short period of time (List of ML indicators, General indicators, Point 1.45).

[21] Specific indicators cover the geographical regions (e.g., offshore jurisdictions), a banking product (loans) and indicators related to several obliged entities.
[22] See Appendix F.
[23] CEO/BEC frauds in particular.

- Stated occupation of the transferor is not commensurate with the level or type of activity, for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area (List of ML indicators, General indicators, Point 1.46).
- Structuring of funds transfers or transactions (List of ML indicators, General indicators, Point 1.47).
- Structuring of gambling purchases, payouts and withdrawals (List of ML indicators, General indicators, Point 1.48).
- The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds (List of ML indicators, General indicators, Point 1.50).
- Using false documents (List of ML indicators, General indicators, Point 1.60).

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

- International funds transfers to a high-risk jurisdiction (List of ML indicators, General indicators, Point 1.18).
- Multiple customers conducting international funds transfers to the same overseas beneficiary (List of ML indicators, General indicators, Point 1.23).
- Multiple funds transfers which appear to be linked to common beneficiaries (List of ML indicators, General indicators, Point 1.26).
- The transaction has no rational purpose (clear and relevant) economic or business (List of ML indicators, General indicators, Point 1.54).
- The transaction is not economically justified, given the business and profession of account holders (List of ML indicators, General indicators, Point 1.55).

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, FIU-K and/or other competent authorities may wish to consider improvements in the way in which 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.

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 FIU-K and other competent authorities' tasks and powers.

- The FIU-K should consider including in their list of indicators also indicators related to other 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 and the relevant AML/CFT regulatory/supervisory bodies, should be involved.

- The AML/CFT Law should extend the reporting entities' obligation to supplement the FIU-K list of indicators with specific indicators related to their sectors/institutions to cover transactions/activities with funds that are proceeds of any criminal offence[24].
- The FIU-K definition (Paragraph 1 of Article 4 of the AML/CFT Law), the FIU-K power to temporary freeze a transaction (Article 27 of the AML/CFT Law) and obligation to provide feedback to obliged entities on reported suspicious transactions (Article 39 of the AML/CFT Law) should be extended to cover also situations, where FIU-K suspects that an online fraud or another criminal offence (e.g., predicate offence for money laundering) has been committed, or attempted, with no suspicion of money laundering or terrorist financing whatsoever.
- FIU-K, 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 frauds and money laundering that the competent authorities may consider including in the list of indicators for suspicious transactions. In this regard, the FIU-K 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.

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

- 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.

[24] And not just those related to money laundering or terrorist financing, as it is currently regulated in Paragraph 2, Point 7 of Article 17 of the AML/CFT Law.

- Significant language errors or unusual content are identified in e-mail or fax communication between the bank and its client or in the documents presented to the bank by its client.
- The client is ordering a payment to be made to a beneficiary only communicates with the beneficiary via e-mail.
- The total turnover of the account changes suddenly and significantly as compared to the account's long-term average.
- Funds for goods/services are refunded onto a credit card other than the one used to make the original purchase.
- A credit card is issued in an offshore jurisdiction or in a high-risk country and used to withdraw funds from the ATM in Kosovo*.

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 differs.

Indicators related to remittance services:

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

6 Appendixes:

A. Agenda of the assessment mission of guidelines to prevent and detect/identify online crime proceeds, 19 – 20 June 2017, Pristina, Kosovo*: https://rm.coe.int/3156-35-iproceeds-assessment-guidelines-for-private-sector-kosovo/1680728334
B. Cybercrime profile – Kosovo*.
C. Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing, Official Gazette of the Republic of Kosovo*, No. 18, dated 15 June 2016: http://fiu.rks-gov.net/legistlation/?Lang=en
D. The FIU-K List of Indicators for Prevention of Money Laundering: http://fiu.rks-gov.net/publications/?lang=en
E. The FIU-K List of Indicators for Prevention of Terrorist Financing: http://fiu.rks-gov.net/publications/?lang=en
F. Typologies of Money Laundering and Terrorist Financing in the Republic of Kosovo: http://fiu.rks-gov.net/wp-content/uploads/2014 /10/Typology-Eng1.pdf
G. Criminal Code of the Republic of Kosovo No. 04/L-082, Official Gazette of the Republic of Kosovo*, No. 19, dated 13 July 2012: http://fiu.rks-gov.net/wp-content/uploads/2014/12/Criminal-Code-of-the-Republic-of-Kosov-Code-No.04-L-082.pdf