iPROCEEDS

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

Version 17 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

Turkey

Project: iPROCEEDS

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1 Introduction

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

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

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

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

1.1 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

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

[2] See FATF Recommendation 34.

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

1.2 Methodology

In preparing this report, the Council of Europe experts have conducted desk review of all relevant AML/CFT legislation and other documents related to this topic and made use of data and information gathered during the on-site assessment mission to Ankara, Turkey on 25th-26th May 2017, where they met with representatives of all relevant institutions.[3]

1.2.1 Meetings

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

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

The delegates represented the following agencies:

- Financial Crimes Investigation Board – MASAK (Ministry of Finance);
- National Cybercrime Department, Turkish National Police;
- Banking Regulation and Supervision Agency;
- Banks and the Banking Association;
- Capital Markets Board;
- Capital Market Association;
- Insurance Association; and
- Undersecretariat of Treasury.

1.2.2 Research

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

- To find out if the current anti-money laundering and countering financing of terrorism (AML/CFT) legal framework related to detection and reporting of suspicious transactions meets the international AML/CFT standards.

[3] The agenda of the meetings is provided in Appendix A.

- To assess if the AML/CFT legal framework provides a sufficient legal basis for updating the existing indicators for suspicious transactions to cover also the prevention/detection of online fraud and online money laundering.
- To evaluate the current list of indicators for suspicious transactions in order to identify if some of the indicators can be used also for prevention/detection of online fraud and online money laundering.

To this end, the relevant provisions of the Law on Prevention of Laundering Proceeds of Crime (AML Law)[4], the Turkish Criminal Code[5], the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (hereinafter referred as Regulation 1)[6], the Regulation on Program of Compliance with Obligations of AML/CFT (hereinafter referred as Regulation 2)[7], the Regulation Regarding the Examination of Money Laundering Offence (hereinafter referred as Regulation 3)[8], and six MASAK Suspicious Transactions Reporting Guides[9] have been analysed and reviewed. In the assessment provided below, the 2007 Financial Action Task Force – FATF mutual evaluation report (MER) on Turkey[10], the 2014 FATF Follow-Up Report on Turkey[11] 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.[12]

1.3 Summary

The information provided by all institutions was informative and gave an overview of the position in Turkey. Relevant points include the following:

- MASAK indicated that it is competent to enforce current and new legislation relating to anti-money laundering and terrorist financing through its mandate and operational activity. MASAK provided an impressive list of capabilities and achievements, where it had used legislation and investigation skills to achieve many of its regulatory requirements.
- MASAK also receives requests from prosecutors and denunciations from other public entities under which requests for information and activity are made. Such requests may be about a person who is under investigation for a criminal offence and relevant information is sought for a prosecution.
- When submitting suspicious transaction reports (STRs), the reporting entities may refer to a list of indicators, but are not obliged to do so. The indicators are seen as guidelines and as such the reporting entities have to describe their suspicions in detail. This provides MASAK an opportunity to review any report and to identify the most appropriate indicators by using key words and professional analysis of the document(s).
- The delegates explained that the Turkish financial sector has been rapidly growing and attracting tremendous amounts of foreign direct investment.

[4] See Appendix C.
[5] See Appendix D.
[6] See Appendix E.
[7] See Appendix F.
[8] See Appendix G.
[9] See Appendix H.
[10] See Appendix I.
[11] See Appendix J.
[12] See Appendix B.

Banking, which has been leading this growth, saw its asset size grow to over 2.3 trillion Turkish Lira (0.58 trillion Euros) by the end of 2015[13].

- The delegates indicated that whilst the size of the banking sector shows growth, the banks are acutely aware of the threats of cybercrime and money laundering.
- The Banking Regulation and Supervision Agency identified the need for significant training and the implementation of computer systems to prevent and detect cybercrime, money laundering and terrorist financing. The Banking Regulation and Supervision Agency reported that they face a high level of threat from cyber criminals, including international attackers. Consequently, every bank has compliance officers and departments that aim to prevent, detect and report cybercrime, money laundering, proceeds of crime and the financing of terrorism to MASAK and other competent authorities.
- There are no unified organisational structures to deal with cybercrime; usually, cybercrime and cyber security are managed by the respective banks' Information Security or Anti-Fraud departments.
- PayPal and Western Union are not licenced to operate in Turkey.
- Coordinated meetings between banks, the Turkish National Police and the Turkish Computer Emergency Response Unit occur regularly. However, it was recognised that there was an inclination for the banks to keep information inside. Banks share information between one another on a medium identified as the SABAS system.
- Virtual currencies are not regulated in Turkey; there is no strategy in place to change that position. The Banking Regulation and Supervision Agency has issued a warning to all banks and payment institutions about the risks related to financial transactions involving virtual currencies. Bitcoin exchangers are subject to investigation under MASAK. However, there is no singular unit responsible for regulating exchangers of virtual currencies.
- The use of customer profiling including the identification of regular types and times of transactions can identify suspicious or fraudulent transactions, where the credit card can be seized by the ATM.
- The Banks Association indicated that fraud and money laundering prevention systems include the implementation of software into the banking IT systems to identify transactions that are not in line with the customer's profile. A buffer time is in place to stop the transaction and allow fraud-monitoring functions to be completed. This gives the bank sufficient time to make further enquiries (including calling the customer by telephone) before a compliance officer decides to stop or allow the transaction.
- The Banks Association indicated that crime prevention and awareness messages are shared with banking customers to identify the risks of social engineering, phishing emails and fake websites. The removal of fake websites has limited benefits because it is often an intensive task that once a site is removed, it simply reappears moments later elsewhere on the Internet.
- The Banks Association reported that active investigation techniques into the opening of accounts, which may be used to launder money, are in place. Where suspicious accounts are identified, they are closed and the details used in the account creation are shared with other banks and are blacklisted to prevent the same details being used elsewhere.

[13] http://www.invest.gov.tr/en-US/infocenter/publications/Documents/FINANCIAL.SERVICES. INDUSTRY.pdf

- The Banks Association indicated that all banks are using MASAK indicators; however, not all of the banks are sufficiently supported by their software to identify suspicious transactions.
- The use of mobile banking applications is seen as a good method of fraud prevention. While mobile devices are subject to attacks, it was identified that the prevention of fraud by such applications significantly outweighs the losses made by such attacks.
- In relation to the online attacks of merchants and other services where large numbers of customer information including credit card account details are obtained, the delegates indicated that banks unilaterally undertook work to identify a common point of compromise. However, there was no information sharing of transactions to identify the points of compromise similar to those that occur in other jurisdictions with a large banking sector (for example Financial Fraud Action UK[14]).
- It was reported that there is sufficient knowledge of AML/CFT amongst employees that work in the Capital Market. The system meant that trust is normally accepted, because money is normally paid from the client's bank accounts and the capital market players relay heavily on banks to conduct the customer due diligence (CDD). The main reason for submission of STRs in this sector was that the source of funds was almost solely sent from another country.
- No cybercrime or online money laundering was detected in insurance sector and among the foreign exchange dealers. The insurance companies are offering insurance against cybercrime attacks, yet no damages were claimed so far.

2 Legislation

The Criminal Code criminalises the computer-related fraud in Articles 158/1f and 243/2, other cybercrime offences are prescribed in the Criminal Code[15] and in the Law No. 5846 on Intellectual and Artistic Works[16]. These offences are generally in line with the Budapest Convention on Cybercrime.[17]

The money laundering offence is set out under Article 282 ("*Laundering of Assets Acquired from an Offence*") of the Criminal Code and, as regards the predicate offences, it is based on *"a threshold"* approach[18]. According to the FATF MER and the FATF 15th Follow-up report on Turkey, the criminal offence of money laundering is not fully compliant with the relevant AML/CFT international standards.[19]

The reporting of suspicious transactions is regulated in Paragraph 1 of Article 4 of the AML Law, which reads as follows:

[14] See https://www.financialfraudaction.org.uk/about-ffa/
[15] There are many other offences within this statute, where the criminal use of computers and computer programs are legislated for. See for example Articles 244, 245 and 245/A.
[16] See http://www.telifhaklari.gov.tr/resources/uploads/2015/10/26/Law%20on%20Intellectual%20and %20Artistic%20Works%20No.5846.pdf).
[17] See the Council of Europe Cybercrime legislation – Country profile - Turkey.
[18] In Turkey only offences which carry a minimum penalty of six months imprisonment are predicate offences for money laundering. All relevant cybercrime offences are covered with this provision. See the FATF 2007 MER on Turkey, pages 25-31, and the FATF 15th Follow-up Report on Turkey, pages 7-8.
[19] Ibidem.

"(1) In case that there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the obliged parties, is acquired through illegal ways or used for illegal purposes, these transactions shall be reported to MASAK by the obliged parties."

In Paragraph 3 of the same article it is also stated:

"(3) Activities of obliged parties required reporting and principles and procedures of reporting shall be determined by regulation."

The reporting obligations are further described in the Regulation 1, which in Article 27 contains almost identical provision on reporting of suspicious transactions related to proceeds of crime. In addition, it also requires reporting of transactions related to financing of terrorism. In paragraph 2 of this Article it is stated "*suspicious transactions shall be reported to MASAK regardless of the amount*". Moreover, paragraph 3 of the same article determines that "*when necessary, multiple transactions shall be taken into consideration together in order to determine whether there is suspicion or a reasonable ground to suspect*".

The Regulation 1 in Article 28 also requires obliged entities to "*take into account, when filling in the STR, the information and findings obtained from an inquiry that they carried out, if necessary, to the extent of their authority and capability*".[20] In paragraph 4 of the same article the Ministry of Finance is authorised to determine for each obliged entity principles and procedures for filling STRs, and in paragraph 5 it is stated that MASAK may prepare guidelines for reports.

The analysis of these provisions shows that the obligation to report covers not just cases of money laundering and terrorist financing but also cases related to transactions with funds that are related to other criminal activities, including the online fraud. It can therefore be concluded that these provisions are fully compliant with the Financial Action Task Force (FATF) Recommendation 20[21] 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[22], which require reporting to the Financial Intelligence Unit any suspicion that the funds are the proceeds of criminal activity, or are related to terrorist financing. This has been confirmed also by the FATF, which in its 15th Follow-up Report on Turkey states that all material deficiencies previously identified with regard to the implementation of FATF Recommendation 13[23], were addressed to a satisfactory level.[24]

---

[20] Similar provision is contained also in Article 19 of the Regulation 2 which describes duties, powers and responsibilities of compliance officers in certain financial institutions.
[21] See the FATF 2012 Forty Recommendations (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html).
[22] 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).
[23] In the previous version of the FATF Recommendations, upon which Turkey was assessed by FATF, the recommendation 13 dealt with the reporting of suspicious transactions. This is now prescribed in recommendation 20.
[24] See the FATF 15th Follow-up Report on Turkey, pages 14-15.

Based on these provisions, in 2014 and 2016 MASAK issued Suspicious Transaction Reporting Guides for the following six sectors:

- Banks,
- Bureaus de Change,
- Insurance and Pension Companies,
- Capital Market Intermediaries,
- Factoring, Financing and Leasing Companies, and
- Other Incumbents.

These guides include lists of indicators for recognising suspicious customers and transactions related to the proceeds of crime and financing of terrorism.

Regarding the MASAK powers, the AML/CFT Law and the above-mentioned bylaws regulate differently situations where MASAK suspects that money laundering or financing of terrorism has taken place from situations where it suspects that (only) other criminal offences have been committed.

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

- Article 7 of the AML/CFT Law which regulates all legal and natural persons' obligation to provide information and documents based on MASAK's request.
- Article 9 of the AML/CFT Law which authorizes MASAK to establish an access system to the data processing systems of public institutions and organisations.

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

- Article 17 of the AML/CFT Law which regulates the seizure of assets.
- Article 19 of the AML/CFT Law which determines MASAK's duties and powers, including the obligation to collect data, receive STRs and analyse them (point e), and to send its reports to the Public Prosecutor's Office (points g, h and i).
- Article 19/A of the AML/CFT Law which authorizes the Minister of Finance to suspend a transaction for 7 working days.
- Article 3 of the Regulation 3 which defines "*examination*"[25], and Articles 7 and 7/A of the same bylaw which determine the working principles of examiners.
- Article 11 of the Regulation 3 which authorizes MASAK or examiners to request for seizure of assets.
- Article 13 of the Regulation 3 which regulates the drafting of money laundering examination report.

In practice, this means that where a suspicious transaction related to an attempted online fraud is reported by the bank to MASAK, the latter is formally not permitted to request a seizure of assets involved in the transaction, nor can the Minister of Finance suspend such transaction. Moreover, it seems that in such cases MASAK or an

[25] According to this provision the "Examination means research and examination works conducted by examiners in order to detect serious findings which indicate that laundering offence has been committed."

examiner is also not allowed to send a report with the findings to the Public Prosecutor's Office.

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 and case studies presented during those meetings.

In 2016, MASAK received 132.494 STRs and 6.419 requests for information and denunciations from the Prosecutor's Office. Examination of the suspicious transaction reports show that between January and October 2016, 16.162 STRs related to cybercrime, of which nearly 8.400 STRs were analysed and 53 reports (related to 543 STRs) were sent to the competent law enforcement authorities. The brief details of some cases are summarised here:

Typology 1:

- An unemployed person opened accounts in 13 different banks to conduct payments related to illegal betting houses.
- Investigations demonstrated that the person was a member of an online gambling network.

Typology 2:

- Three persons received significant amounts of money and successfully withdrew over one million EUR in cash.
- MASAK were alerted and successfully blocked 100.000 EUR.
- Investigations subsequently proved that the three men were members of an online gambling syndicate.

Typology 3:

- Analysis of suspicious transaction reports allowed MASAK to identify an illegal pyramid scheme involving the use of electronic currencies.
- Evidence included on-line announcements and false promises to victims, which enticed them to invest money that was subsequently defrauded from them.

The Banking Regulation and Supervision Agency reported that organised criminals operating inside and outside of Turkey often undertake cybercrime attacks against banks. Threats that exist (but are not limited to) include the following typologies:

- Credit card fraud.
- Social engineering attacks including "CEO fraud[26]" and calls to customers from persons purporting to be the bank in an attempt to gain information as well as persuade them to transfer money to the criminal accounts.
- Online gambling.
- Fraud – general types of offending.
- Fraud – specifically where criminals sell non-existent electronic money by offering a digital code in lieu of goods or services online.
- Malware – specifically malicious software employed against banking applications on Android mobile telephones.

The delegates identified that large amounts of the criminal proceeds obtained through online betting are transferred to Northern Cyprus (where gambling is legal).

The Banking Association of Turkey explained that the banks are familiar with a diverse range of threats that are active in the country which include fraudsters, organised criminals and cybercriminals. Matters that were most relevant to this report and were identified as serious risks included social engineering attacks, credit card fraud, money mules and Internet banking attacks. The Banking Association described relevant methods of attack of these different typologies:

Typology 1: Social engineering attacks
- Criminals calling customers purporting to represent the bank (or the police, Prosecutors, insurers or a law firm) in order to obtain private information or login information and defraud the customer or bank.
- Phishing emails purporting to be from the bank to customers often with malware attachments.
- Fake websites offering loans or credit and asking for advanced payments, which were normally linked to a new or current banking product.
- CEO fraud.

Typology 2: Credit card fraud
- Point of Sale attacks (often committed by employees abusing trust and interfering with devices).
- Automated Teller Machine (ATM) attacks including machine overlays and other physical interferences of the activity of ATM machines.
- Card-Not-Present fraud, where a customer's credit card data has been obtained through a Cybercrime act against a merchant.

Typology 3: Money mules
- The creation and use of newly opened personal accounts.

[26] CEO fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorised wire transfers, or sending out confidential information.

- The establishment of companies and bank accounts, which remain dormant for a short period before money is paid into the accounts and is either cashed out or moved to overseas accounts in a short time.

Typology 4: Internet Banking Attacks

- Malicious Software attacks against customers and the banks.
- Mobile platform attacks. A significant proportion of banking has now moved to banking applications. The creation of false applications and malware, particularly in Android devices is a risk.

4 Indicators

As mentioned above, the indicators for suspicious transactions were adopted by MASAK and are provided in six Suspicious Transaction Reporting Guides. In the introductory part, the objectives and the scope of these guides are described as follows:

- The guides provide information on the processes of making suspicious transaction reports on paper or electronically, and presents detailed information on how to complete STRs.
- The guides distinguish between the normal STRs and STRs with deferment request[27].
- The guides in the suspicious transaction reporting form inter alia encourage obliged entities to indicate the suspected illegal activities in the acquisition of financial assets that are subject to the suspicious transaction. To this end, the guides provide also a list of criminal offences ("*Criminal Suspicious Categories*") that includes Cybercrimes. Moreover, the reporting form under a title "*Transaction Channel*" contains also channels such as ATM, Internet, POS and telephone.
- The indicators for suspicious transactions are for guidance only and shall not be disclosed in the reporting form. The obliged entities shall not restrict themselves to the indicators provided in the guides and shall file the STR even if the suspicious transaction does not conform to any of listed indicators.

The indicators included in all six guides are divided as follows:

- Indicators based on client profile and transactions[28];
- Indicators related to sectors' specific transactions;
- Indicators related to terrorist financing or transactions with high-risk countries; and
- Indicators related to non-profit organisations.

The analysis of indicators shows that they include transactions with virtual currencies. E-money, credit cards, mobile phones, and certain transactions conducted via Internet. While there are no specific indicators covering the online fraud[29] and/or online money

[27] Such requests may only be sent to MASAK when there is information on strong indicators beyond a mere suspicion which support the suspicion that the asset is linked to laundering of proceeds of crime or financing of terrorism.

[28] These indicators could be considered as "general indicators" since they are included in the guides for all six sectors.

[29] CEO/BEC frauds in particular.

laundering, some of the existing indicators have been identified that can also assist obliged entities in preventing/detecting these types of criminal behaviour. 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.

a) Indicators applying to the suspect's account:

- There is no reasonable correlation between the client's job/occupation, assets, and transactions (STR Guide for Banks, Code T-001-1.4).
- Client does not or cannot explain the source of the asset that is involved in the transaction (STR Guide for Banks, Code T-001-3.3).
- Client attempts to open an account, make a transaction or act on behalf of others and make transactions in their accounts without submitting identification, or under false or assumed names without a valid identification document (STR Guide for Banks, Code T-001-3.12).
- Client's account activity shows cash deposits and withdrawals that are incompatible with client's standard of living, occupation or income (STR Guide for Banks, Code T-001-3.18).
- Funds in an account understood to be opened for the purpose of withdrawing funds transferred from abroad are always withdrawn in cash, or the account remains inactive for a long time after a period of such transactions (STR Guide for Banks, Code T-001-3.20).
- Transfers are made to or from high-risk countries or offshore locations in significant lump sums or small amounts in frequent transactions that cumulatively become significant over a period of time without a reasonable explanation. (STR Guide for Banks, Code T-001-3.28).
- Electronic fund transfers from high-risk countries or in significant amounts or frequency do not contain a reasonable explanation pertaining to their purpose, have incomplete principal and beneficiary names or addresses in transfer messages, or contain aliases, abbreviations or codes in lieu of these (STR Guide for Banks, Code T-001-3.29).
- The client makes domestic or international electronic fund transfers in a significant amount or frequency that is incompatible with the known job and activity, sources of income and wealth of the client (STR Guide for Banks, Code T-001-3.30).
- Accounts are opened for the sole purpose of transferring funds abroad; there is little or no information about the relationship between the transferor and recipient of funds (STR Guide for Banks, Code T-001-3.33).
- Client frequently transfers funds to electronic currency companies for purchasing electronic currency in amounts that are not compatible with client's living standard and income level (STR Guide for Banks, Code T-001-3.46).
- Client frequently transfers funds to online goods/services purchasers and sellers in amounts that are not compatible with client's income level and living standards (STR Guide for Banks, Code T-001-3.48).
- Client's account has no activity other than receiving funds from an account abroad, and withdrawal or transfer of the funds to another account (STR Guide for Banks, Code T-001-3.49).
- Frequent and small transfers to mobile phones (STR Guide for Banks, Code T-001-3.57).
- Client makes regular transfers to their own mobile phone (STR Guide for Banks, Code T-001-3.58).

- A large number of senders transfer funds to a single recipient's mobile phone (STR Guide for Banks, Code T-001-3.59).
- A large number of transfers received via a mobile phone number are withdrawn from ATMs within a short period of time (STR Guide for Banks, Code T-001-3.60).
- Funds transferred from or via high-risk countries are transferred to third parties shortly thereafter (STR Guide for Banks, Code T-001-4.05).
- The online branch of the intermediary is accessed by the same IP address to perform transactions about different clients who are unrelated to each other (STR Guide for Capital Market Intermediaries, Code T-002-3.8).

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

- Client has business or other relationships with high-risk persons or entities (STR Guide for Banks, Code T-001-1.5).
- The transaction has no reasonable and ordinary financial or legal basis or justification (STR Guide for Banks, Code T-001-2.3).
- Credit card customers repeatedly draw significant amounts of cash; cards are frequently and/or unreasonably used for purchasing gold and other easily convertible goods (STR Guide for Banks, Code T-001-3.44).
- Client transfers funds to bitcoin brokers for purchasing bitcoins (STR Guide for Banks, Code T-001-3.47).
- Funds are sent to or received from high-risk countries; client opens accounts in or uses credit cards issued by financial institutions in high-risk countries (STR Guide for Banks, Code T-001-4.03).

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, MASAK 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 MASAK's and other competent authorities' tasks and powers.

- MASAK should consider improving the current lists of indicators, and in particular those indicators that related to all 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 authorities should consider extending the MASAK's and/or other competent authorities' powers:

- to request seizure of assets (Article 17 of the AML/CFT Law and Article 11 of the Regulation 3);
- to collect data, receive STRs and analyse them, and to send reports to the Public Prosecutor's Office (Article 19, points g, h and I of the AML/CFT Law); and
- to suspend a suspicious transaction for 7 working days (Article 19/A of the AML/CFT Law);
- to cover also situations, where there is a suspicion 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.

- The authorities should consider amending Article 3 of the Regulation 3, which defines "*examination*"[30], and Articles 7 and 7/A of the same bylaw, which determine the working principles of examiners, to cover also situations, where there is a suspicion 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.
- 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

These sections present 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, MASAK 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)[31].
- 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.

[30] According to this provision the "*Examination means research and examination works conducted by examiners in order to detect serious findings which indicate that laundering offence has been committed*."

[31] The existing indicator No. T-001-3.47 in the STR Guide for Banks only covers client's transfers of funds for purchasing Bitcoins. The proposed new indicator is wider since it covers all transactions with all types of virtual currencies.

- The client makes withdrawals of funds received from a foreign jurisdiction where the transfer was made near to the close of business in the foreign jurisdiction and the withdrawals are made after close of business, particularly after close of business on Friday, in the foreign jurisdiction.
- Significant language errors or unusual content are identified in e-mail or fax communication between the bank and its client or in the documents presented to the bank by its client.
- The client ordering a payment to be made to a beneficiary only communicates with the beneficiary via e-mail.
- The total turnover of the account changes suddenly and significantly as compared to the account's long-term average.
- Funds for goods/services are refunded onto a credit card other than the one used to make the original purchase.
- 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, 24th-25th May 2017 Ankara, Turkey: https://rm.coe.int/3156-35-iproceeds-assessment-guidelines-for-private-sector-final-turke/1680716960
B. Cybercrime legislation - country profile – Turkey
C. Law No. 5549 on Prevention of Laundering of Proceeds of Crime, Official Gazette No. 26323, dated 18/10/2006: http://www.masak.gov.tr/en/content/l-p-c-national-legislation/159
D. Criminal Code No. 5237, Official Gazette No. 25611, dated 12 October 2004; the law was amended with the Law No. 6217, dated 31.03.2011: http://www.lawsturkey.com/law/criminal-code-law-of-turkey-5237).
E. Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, Official Gazette No. 26751, dated 09/01/2008; amended on 18.03.2016: http://www.masak.gov.tr/userfiles/file/REGULATION_1.pdf
F. Regulation on Program of Compliance with Obligations of AML/CFT, Official Gazette No. 27009, dated 26/09/2008: http://www.masak.gov.tr/userfiles/file/REGULATION_2.pdf
G. Regulation Regarding the Examination of Money Laundering Offence, Official Gazette No. 26603, dated 04/08/2007: http://www.masak.gov.tr/userfiles/file/Regulation_Examination_ML(Amended_10_06_2014).pdf
H. MASAK Suspicious Transaction Reporting Guides for Banks, Bureaus de Change, Insurance and Pension Companies, Capital Market Intermediaries, Factoring, Financing and Leasing Companies, and Other Incumbents: http://www.masak.gov.tr/tr/content/sektorel-supheli-islem-bildirim-rehberleri/2358
I. FATF Third Round Mutual Evaluation Report on Turkey: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Turkey%20full.pdf
J. FATF 15th Follow-up Report on Turkey: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Turkey-FUR-2014.pdf