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

Albania

Project: iPROCEEDS

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contents

1 Introduction

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

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

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

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

1.1 Objectives

The main objective of the report is to put forward a set of recommendations for elaboration and/or improvement of guidelines and indicators for financial sector entities to prevent and detect online fraud and money laundering in the online 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, pages 6 and 38 (https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a).
[2] See FATF Recommendation 34.

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 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 Tirana, Albania on 13 March 2017, where they met with representatives of several relevant institutions.

1.2.1 Meetings

Meetings were held with several agencies and industry players:[3]

- The General Directorate for the Prevention of Money Laundering - GDPML (Ministry of Finance);
- The General Prosecution Office;
- The Bank of Albania;
- The Financial Supervision Authority;
- The National Chamber of Notaries;
- The Supervision Authority for Games of Chance;
- Representatives of several banks and the Banking Association;
- Electronic Payment Providers; and
- Money Remittance Providers.

All meetings 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 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:

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

- To find out if the current anti-money laundering and countering financing of terrorism (AML/CFT) legal framework related to detection and reporting of suspicious transactions meets the international AML/CFT standards;
- To assess if the AML/CFT legal framework provides a sufficient legal basis for updating the existing indicators for suspicious transactions to cover also the prevention/detection of online fraud and online money laundering; and
- To evaluate the current list of indicators for suspicious transactions in order to identify if some of the indicators can be used also for prevention/detection of online fraud and online money laundering.

To this end, the provisions of the Law on the Prevention of Money Laundering and Financing of Terrorism (AML/CFT Law), the Minister of Finance Instruction No. 28 on the Reporting methods, procedures and the preventive measures taken by the subjects of the AML/CFT Law (Instruction No. 28), the Minister of Finance Instruction No. 29 on the Reporting methods, procedures of Non-Financial Free Professions (Instruction No. 29) and the Bank of Albania Regulation No. 44 on Prevention of Money Laundering and Terrorist Financing (Regulation No. 44) have been analysed and reviewed. In the assessment provided below, the most recent Council of Europe MONEYVAL Committee mutual evaluation report (MER)[4] on Albania and other documents related to criminalisation of online fraud and other criminal offences mentioned in the Budapest Convention on Cybercrime have also been taken into account.[5]

2 Legislation

In Albania, all criminal offences envisaged under the Budapest Convention on Cybercrime, including the computer-related fraud, are included in the Criminal Code.[6] According to the MONEYVAL 2011 MER on Albania and the MONEYVAL 6th Regular Follow-Up Progress Report on 4th Round Mutual Evaluation of Albania, the criminal act of money laundering (Article 287 of the Criminal Code) is based on "*all crime*" approach[7] and is criminalised largely in compliance with the relevant AML/CFT international standards.[8]

The reporting of suspicious transactions for all obliged entities is regulated in Paragraph 1 of Article 12 of the AML/CFT Law[9], which reads as follows:

"1) Subjects submit a report to the "Responsible Authority", in which they present suspicions for the cases when they know or suspect that laundering of the proceeds of crime or terrorism financing is being committed, was committed or attempted to be committed or funds involved derive from criminal activity…."

[4] See MONEYVAL 2011 Report on Fourth Assessment Visit to Albania (https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715a9f).

[5] See the Council of Europe Cybercrime legislation - country profile, Albania (Appendix B).

[6] Ibidem.

[7] This means that all criminal offences, including cybercrime related offences, are predicate offences for money laundering.

[8] See MONEYVAL MER on Albania, pages 62 – 75, and MONEYVAL 2015 6th Regular Follow-Up Progress Report, page 7 (https://rm.coe.int/6th-regular-follow-up-progress-report-4th-round-mutual-evaluation-of-a/1680715a9e).

[9] A very similar provision is provided also in Article 11 of Instruction No. 28 and in Article 10 of Instruction No. 29.

The analysis of this provision 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. It can therefore be concluded that this provision is fully compliant with the Financial Action Task Force (FATF) Recommendation 20[10] and Article 33 of 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 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 does not contain a definition of suspicious transaction nor does it provide any further guidance regarding the adoption and implementation of indicators for recognising suspicious transactions. Similarly, both instructions are silent in this regard and only provide in Annexes the SAR and CTR reporting forms for financial institutions and designated non-financial businesses and professions (DNFBPs).

Further analysis of AML/CFT bylaws and regulations provided by the Albanian authorities has revealed that so far, the indicators were only issued by the Bank of Albania. In Annex 1, attached to the Bank of Albania Regulation No. 44, the "Guideline to measure risk arising from ML/TF" is provided, which in Section 6 contains an extensive list of suspicious indicators. According to Article 3, this Regulation, including the Annex 1 with suspicious indicators, only applies to banks and other financial institutions that are licensed and supervised by the Bank of Albania.

It is clear from the above that the legislative framework already requires the obliged entities to report to GDPML any suspicion of criminal activity or attempted criminal activity, including online fraud and online money laundering. However, on the recipient's side the AML/CFT Law limits the powers of GDPML, so that they can only be used for the purpose of preventing money laundering and terrorist financing. This applies not only to the GDPML's powers to suspend suspicious transactions (point (g) of Article 22) or order the monitoring of bank transactions (point (l) of Article 22), but also to GDPML's authority to request data from the obliged entities (point (c) of Article 22) and to send their reports with the analysis to the General Prosecutor's Office and other competent law enforcement authorities (point (e) of Article 22).[12]

[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).

[12] In practice, this means that if an attempted online fraud is reported by the bank to GDPML, the latter 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 limits the exchange of information with these authorities only to cases of ML and TF.

3 Typologies and selected case studies

As mentioned in Section **Error! Reference source not found.**, meetings were held ith 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 the meetings.

3.1 The General Directorate for the Prevention of Money Laundering - GDPML (Ministry of Finance)

The General Directorate for the Prevention of Money Laundering - GDPML is the Albanian Financial Intelligence Unit (FIU). Together with the Prosecution and the Sector for investigation of money laundering at the Directorate for investigation of economic and financial crime of the Albanian State Police they have a mandate to counter money laundering and terrorism financing. GDPML acts as an administrative type of FIU and its powers are similar to powers of other FIUs of the same type.

The GDPML reported the following in relation to cases and typologies:

Typology: Business Email Compromise (BEC)

- BEC is the main cybercrime risk that is observed by GDPML. Banks often accept payment instructions by email and businesses are not aware of the risks presented by that medium.
- Since email messages are relatively easy to spoof and email systems relatively easy to break into, several Albanian businesses have fallen victim to this fraud.
- In most cases the fraudsters convince the victim to make payment into an account under their control, after sending falsified emails pertaining to originate from a known supplier or other party, asserting changed account details.
- BEC attacks are targeted. In one example, a BEC attack was executed precisely when a target’s son had died – and played on this event to increase chances of success. This makes countering this fraud difficult.
- The fraud often only becomes obvious after a report is filed and analysis is performed.

- Banks do not carefully check the name of the sender and destination account of payment instructions. This is especially true for foreign names and accounts. This increases the risk of fraudulent transactions going undetected (which often use similar, but slightly differing names) and being processed successfully.
- In total, GDPML has detected about 50 cases of BEC fraud, with an average value of EUR 60K to EUR 100K. In one case, the amount was well over EUR 700K. In all cases Albanian businesses (and not individuals) were targeted. The target is usually compromised via email. In many cases the fraud involved registering a company or domain name similar name to a supplier of the target company.

As a policy approach GDPML always maintained that tackling this issue is part of banks' reporting obligation and their duty of care towards their customers; especially since several banks were able to prevent similar cases. An unofficial translation of the letter to banks outlining GDPML's policy is attached as Appendix D.

Due to the targeted nature of these attacks, reporting BEC incidents takes victims long time. On average reports only reach authorities in two to three days after the fact. In another example, € 1 Million worth of funds were disbursed to Hungary and withdrawn in cash there. It has proven difficult to freeze and seize money in such cases - even if a request to do so was sent to foreign counterparts on the same day that the fraud was discovered. In this example, Hungary had issued a freezing order but it came into force only after the money was gone.

Although cases of BEC are happening in Albania, only few requests related to such frauds were received from counterparts. Albanians and Albanian businesses, in other words, mainly appear to be victim of this fraud, whilst perpetrators are mainly foreign.

GDPML has imposed a fine for late reporting of suspicious transactions in these cases and subsequently emphasised the importance of customer due diligence and reporting in a meeting with the Albanian banks. After the initial meeting and fine, better reporting was observed. It is still possible, however, that not all cases are reported to GDPML. One issue is that failed attempts of BEC fraud and associated but failed transactions are possibly not reported.

GDPML currently see a reduction in fraud schemes and in money values involved. This could well be related to their intervention in 2016. Statistics over that year were not available at the time of writing of this report; however BEC cases may also be reported to the police and may then arrive to GDPML through their police contacts. Combined statistics (police and GDPML) on cybercrime (or BEC) are not available.

Fraudulently disbursed funds were mostly destined to countries in Latin America, such as El Salvador, Ecuador, Panama) and Europe (Hungary, Czech Republic, Cyprus and Ireland were encountered).

Perpetrators of BEC fraud are not always identified. GDPML mainly rely on law enforcement authorities for this. Also, they do not receive feedback on the outcome of

investigations conducted by the Albanian Police. They only know of one case where the fraud was successfully stopped.
Amendments are on the way that will provide for an obligation for banks to check that the IBAN code and name in any payment instruction are checked thoroughly and that any transaction where there is a deviation from the name associated with the IBAN code is either declined or meticulously verified.

Possible indicators of fraudulent use of banking facilities include:

- The mismatch of IBAN and name of the account,
- The rapid opening of an account, followed by immediate, high value transactions. In the example case mentioned, there was only one day between opening of the account and the reception of significant fraudulently obtained funds.
- Large sums in an account that would be suspicious in Albania – by virtue of the low average transaction value.

For all these cases, due diligence on the clients account usage is important to detect perpetrators.

3.2 The General Prosecution Office

The General Prosecution Office (GPO) reported on several relevant typologies:

Typology 1: BEC

- BEC frauds often involve foreign counterparts, mainly in Far East countries.
- The fraudsters generally hide their tracks using one or several money transfers.
- The victims are often instructed to use remittance services.
- Third persons are often employed abroad to receive moneys as mules.
- Suspect countries are typically countries that Albania has significant difficulty with in terms of cooperation. As a result, investigations into these crimes are usually not very successful. In BEC cases it is often extremely hard to find a perpetrator. In part because many foreign jurisdictions do not provide adequate information – even if cooperation is otherwise efficient. In an example case related to the UK, the Albanian prosecution did not get any reply despite using the proper (MLA) channel.

Typology 2: Attacks against banks

- Several types of bank fraud were detected, both due to hacking of bank systems as well as fraud by insiders.
- Reporting such crimes to the police or prosecution (and often as STR) is mandatory, but in practice, reporting does not appear to always take place.
- According to the prosecution, there appears to be an issue with communicating with banks, because they seem reluctant to report fraud that took place in relation to their systems.
- The prosecution suspect that banks are afraid of reputational risk and may hence not be reporting all cases.

- Moreover, when the bank is a victim, they usually cover the losses for the related account holders.
- There is little known about these cases, except that when there is theft by bank employees, punishment is often severe.

Typology 3: Credit card cloning

- Card details are fraudulently obtained through purchasing online, hacking, malware or other vectors.
- Cards are cloned onto blank cards.
- Cloned cards are used for cash withdrawals or used to make purchases on POS systems in general retail.

When such fraudsters are arrested, the prosecution try to seize the cash, cards or goods involved at the time of arrest of the suspects.

Apart from these cases, also child pornography cases and ID theft are common, the latter often related to impersonation on social media. These do not often have a financial motive. In cases of ID fraud and child pornography there is no practice of investigating potential money flows and no financial investigation is conducted.

In some of the above-mentioned cases, criminals are known to use gambling to try and launder funds - usually involving sports betting. They use the fraudulently obtained funds to place sports bets. Although this may appear to be related to a gambling habit, at least in some cases, this channel is used to launder money.

Cooperation with GDPML is mainly sought when it is clear that there is a case related to money laundering. The use of GDPML for intelligence purposes needs further development according to the prosecutor.

3.3 The Bank of Albania

The Bank of Albania (BoA) highlighted the threat of internal fraud and reported that banks usually have a competent organisational unit to deal with this threat. Operational risk, such as the risk related to external fraud (cybercrime) or skimming, is not currently the subject of separate regulation, nor is there an organisational unit dealing with it in the BoA. There is a plan to establish such unit in the future. Mere cybercrime and cybersecurity are not a big operational risk for banks especially since the use of online banking is very low.

In the banking system, 10 out of 16 banks use software to do fully automated STRs and indicator processing. Six banks still work manually, and, although they have some software, they do not have fully automated ML/TF detection systems. STRs and CTRs are all sent to GPDML electronically.

Virtual currencies are not regulated in Albania. The BoA policy for this is not entirely clear. At the same time only limited use of virtual currencies is observed in Albania.

Electronic money (e-money) and Internet payment services, such as prepaid cards, are more common in Albania and are regulated. The main purpose for these regulations is to prevent TF and not fraud or ML. E-money is a new development. In 2015 several schemes started, mostly run by non-banks (Vodafone, Visa, Easypay). They support only very limited transaction values of up to EUR 2.500 a year.

The e-money regulation allows for three risk categories. After initial approval of the operators by the bank, a EUR 2.500 limit was put in place to familiarise both the regulator and the e-money operators with the risks and procedures involved.

In relation to BEC it was remarked that in order to prevent BEC the new AML/CFT Law will mandate banks to collect more data on the beneficial owner of the account, especially for non-resident accounts.

In relation to cybersecurity the BoA has issued a separate regulation. It contains generic provisions on protection of bank data and information systems. There will be a registration and management system for operational risk in this area. Data breaches and incidents (also if no money or data is ostentatiously lost) are to be reported at the BoA.

3.4 The Financial Supervision Authority

The supervision tasks of the Financial Supervision Authority of Albania (FSA) focus on three areas:

- Insurance, including life insurance,
- Pension funds, and
- Capital markets[13].

The FSA is also responsible for the supervision of AML/CFT requirements in these markets. In 2015-2016 the FSA issued the AML/CFT manuals and guidance documents for the insurance sector and for pension funds. These documents require obligors to address the ML/TF risk. Illegal gambling is a criminal offence in Albania and the law requires companies to have a written AML/CFT program that includes the application of know your customer (KYC) and customer due diligence (CDD) requirements.

A recent national ML/TF risk assessment revealed that the ML risk of the Albanian insurance and pension funds markets is low. A more common problem in the insurance market is first party fraud. However, since most claims are made in person, risk of fraud is low there too. Cybercrime is not observed in this sector, one example related to foreign electronic investment.

Typology: Foreign (electronic) investment

- Customers are being targeted with investment opportunities online, with offers targeted at the Albanian market.
- This activity requires a license.

[13] There is no stock exchange in Albania and the capital market is therefore not well developed.

- Several parties from abroad are making offers based on foreign licenses that do not cover Albanian territory.
- This is an administrative offence, but hard to enforce against as operators are often relatively anonymous and international cooperation is often slow.

The Serbian branch of an UK licensed operator (with ties to Cyprus) was offering investment opportunities on the Albanian market. They were promoting actively to clients in Albania, although their investigation in Serbia and UK shows that they were only licensed to perform business in the UK.

3.5 The National Chamber of Notaries

Notaries are an obliged entity under the AML/CFT Law and are therefore obliged to report suspicious and cash transactions to GPDML. They also have a retention obligation for minutes of transactions they execute. Although they are aware of the obligation, it is hard to train notaries adequately and teach them to recognise suspicious transactions. In order to improve reports, the Chamber is creating a bureau that will relay all reports to GPDML, and will review them in order to improve reporting quality.

There are 472 notaries in the country and they are all members of the Chamber. The Chamber has trained all of them, together with a GDPML specialist. There are no specific indicators for suspicious transactions for notaries and the Chamber is of the opinion that indicators have a limited value. A notary's personal suspicion is eventually the best indicator. Although several ML typologies were shared during the trainings, all were rather generic and none related to cybercrime. Furthermore, all notaries are required to buy a fingerprint reader to match customer fingerprints with ID card fingerprints. This reduces chances of ID fraud.

Most STR cases are therefore related to foreigners and the following example was provided in this regard: a transaction pertaining to EUR 200k property bought in Albania by a young Russian lady was reported as STR.

Cybercrime is not observed by the Chamber.

3.6 The Supervision Authority for Games of Chance

In 2015 a new law was passed on gambling, which also includes provisions on monitoring online gambling. A process is being implemented for licensing online gambling operations in the next two years. At the time of the visit there was no license issued for online gambling. It does exist all the same, as foreign operators offer services to Albanians from abroad.

The regulator actively monitors gambling websites in cooperation with the National Security Computer Agency (ALCSIRT) and they block sites that do not have an office in Albania. As a result, around 2.000 gambling websites have been blocked. These are not only websites from Albania, but mainly foreign websites that offer service to Albania. Recently new means to directly block sites were implemented without the manual intervention of ALCSIRT. The gambling regulator can now block sites using ALCSIRT’s infrastructure.

Another issue is that these operations circulate money through banks as they have to have payments made to them somehow. Where foreign websites are concerned; payment also usually involves credit cards. The regulator has been in discussion with banks, to prevent such payments. However, this is more a task for GDPML. Indicators for recognising suspicious transactions could also help to counter illegal gambling. The regulator believes more action along these lines would be helpful.

3.7 Banks and the Banking Association

All Albanian banks are a member of the Banking Association (BA). BA has a compliance committee of which three members are heads of compliance in their member bank. AML/CFT issues are a focus area of the compliance committee.

The GDPML and the committee organise a biannual training on AML/CFT. Banks mainly send front office staff to the trainings that are organised. In local branches, managers usually act as AML/CFT officers in the field. Cybercrime issues are not usually treated by the compliance department in Albanian banks. Rather it is seen as an issue for the IT (security) department. In other Albanian banks, it is part of the operational risk department.

Albanian banks only detect very limited numbers of cybercrime. Most crime, according to their representatives, was directed to their clients, and none or very few was in relation to banking systems themselves. So far, fraud cases were only detected by clients and not by ML/TF indicators related software that they operate.

Typologies detected by the members of the BA are mainly related to BEC and credit card fraud.

Typology 1: BEC

- A bank reported nine cases of BEC in the recent past. In these cases, the bank’s front office was detecting an IBAN mismatch: they spotted the changed addresses and detected that there was a mismatch between the country of the account holder and the IBAN, for example.
- These cases did not cause any damage. They were able to stop all of the related transactions and the attempted transactions were subsequently reported.

One bank has a blacklist of IBAN codes that were involved in frauds. If the customer reports a BEC case, for example, the destination IBAN can be listed and further transactions postponed, pending the notification of the authorities (via an STR). It was observed that the use of a black list should perhaps be considered locally, across banks, or even regionally.

Typology 2: Credit card fraud

- Most card fraud is related to Internet purchases.

- These frauds are reported by clients, who are subsequently reimbursed.

Overall limited anti-fraud systems exist, also due to the low usage of e-banking and m-banking. Some banks are looking into this, also in relation to fraud, but none have implemented automated fraud detection at this moment in time.

3.8 Electronic Payment Providers and Money Remittance Providers

Money remittance services are regulated by the BoA. Both MoneyGram and Western Union are present in the market. Recently, also three licenses for e-money were issued to Easy Pay, M-Pesa (part of Vodafone Albania) and M-Pay. All these work by mobile phone. Lastly, Albania's largest card issuer, Paylink, issues credit cards for various financial institutions. They are licensed by the BoA but mainly work as wholesale card issuing provider for the banking sector.

The relevant indicators for these sectors were last updated in 2013, yet no English translation of these was available.

In relation to credit cards a lot of fraud indicators (and detection functions) are provided by Visa and MasterCard as well. These are proprietary and only relate to card transactions. Paylink allows for integration of local fraud indicators for each of the issuers on the platform. For credit card fraud (Paylink), indicators of fraud are often automated:

- The times between card-present transactions in different countries are an important indicator of fraud or skimming.
- 3D secure (MasterCard) and the equivalent Visa system can be used according to the customer Banks own risk appetite.
- Most issues related to credit cards are related to e-commerce.
- Skimming at ATMs has declined due to the advent of EMC (Pin & Chip).
- Overall, credit card is a riskier payment method, especially if higher limits are applied.
- Other, frequently used indicators are unusual transaction values and geographical indicators.
- Albania is relatively less susceptible to credit card fraud due to the lower limits on most cards.

Representatives of the money remittance providers presented their activities related to abuse of remittance services. The following was reported in this regard:

- MoneyGram performs due diligence and further investigate transactions when needed. In case of suspicions they contact the Cybercrime Unit of the Albanian State Police.
- Western Union reports that in addition, they have checks in place to prevent their remittances from being used as (pre)payment for online orders of goods or services as this presents a very high risk (of non-delivery).
- There is also a guideline that prevents use of their service for betting purposes.
- MoneyGram sees advance fee frauds.

In relation to electronic money M-Pesa was the first institution to provide an e-money service in Albania. This required a significant change in law and policy since most regulations were still geared towards the traditional banking sector. They currently have their own ML typologies and have set up their own fraud monitoring platform. For cybercrime, no specific indicators are present.

E-money providers use dedicated software platforms to monitor their services and transactions for fraud and ML risk. Most screening is based on lists and fraud indicators. The services all employ a relatively low transaction limit of EUR 2.500 per year, even though there is no existing obligation to that effect.

A good indicator for ML is the number of parties involved: accounts with only a single destination account and many donor accounts, or an account displaying the opposite pattern (many outbound, one inbound) are often indicative of fraud. Moreover, the use of the account for structured transactions is also a good indicator – the service can be used to hide origin and destination of funds, if a party would succeed in creating many accounts.

GDPML provide only limited feedback on the application of AML/CFT measures within the various sectors. Especially in the new sector of e-money there is a clear need to receive more specific feedback on their performance to reduce risks and improve the quality of reports –also ion relation to ML and online fraud. So far, only limited case studies were provided. A more risk based approach should be taken, according to some parties, since the current AML/CFT regime is very onerous in relation to the low risks that e-money services present in their current form.

So far limited use of these services was observed in relation to cybercrime.

4 Indicators

As mentioned above, the indicators for suspicious transactions for financial institutions were adopted by the Bank of Albania and are provided in Annex 1, Section 6 of Regulation No. 44. In the introductory part of this section the objectives, scope and use of indicators are described as follows:

- The obliged entities shall consider as suspicious indicators the operations which according to their nature may be considered as unusual for the relationship of the business and serve as signs to initiate a risk assessment procedure.
- The indicators aim to assist entities to assess/measure possible signs of ML/TF and to contribute in ensuring the correct and homogeneous accomplishment of the reporting obligations on the suspicious transactions.
- The obliged entities shall assess also other models of behaviour, which are not described in the suspicious indicators.

The BoA reported that the choice to have non-binding indicators was made to allow banks to implement not only a minimal set, but to stimulate them to work out effective indicators themselves. The current list of indicators was prepared in cooperation with the GDPML and the Banking Association.[14] In practice banks use these indicators next to the internal and local indicators they themselves have developed. GDPML asked banks that they disclose the entire indicator list recently. In line with GDPML voluntary implementation policy, banks are actively amending indicators, yet specific indicators for fraud (including online fraud) are lacking.[15]

The indicators are divided in 17 categories and the list of indicators includes money laundering through new methods of payments/electronic products. The analysis shows that there are no specific indicators covering the scenarios related to online fraud and/or online money laundering that have been identified during the on-site assessment mission. Nevertheless, some of the existing indicators have been identified that can also assist obliged entities in preventing/detecting online frauds[16] 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:</u>

- Large transactions frequently with parties, which are recently, established companies and whose activity object is not in compliance with the activity carried out by the customer or which have a general purpose (Annex 1, Section 6, point 2d).
- The payment means appear not in compliance with the risk-transaction characteristics, for example: pre-payment to the new supplier who is at a "high risk" location (Annex 1, Section 6, point 14h).

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

- The customer shows to not have adequate knowledge on the nature, object, amount or purpose of the transaction or relationship or provides non-realistic, confusing or inconsistent explanations, which drive to the suspicion that the customer is acting for a third person (Annex 1, Section 6, point 1h).
- The customer conducts large transactions in cash or through unusual procedures when it is made known that is subject of a penal procedure, preventive measures or commodities sequestration or is in close contact (for example family member) with people to whom these measures are taken, or when the other party of the transaction is subject of these measures (Annex 1, Section 6, point 1k).
- The customer conducts frequent and large transactions, which are inconsistent with his economic profile of the transaction (Annex 1, Section 6, point 1o).
- The customer benefits transfers in his account by different third parties, which are not justified by the nature of his business (Annex 1, Section 6, point 1p).
- Large-amount transactions by persons, who do not conduct any economic activity or are in economic difficulties (Annex 1, Section 6, point 2k).
- Cash deposits and withdrawals at large amounts which are not justified accordingly the economic profile of the customer's transactions (Annex 1, Section 6, point 3a).

[14] The law enforcement authorities are typically not involved in development of these indicators.
[15] Typologies of fraud schemes are not commonly shared either.
[16] BEC frauds in particular.

- Large cash withdrawals from a previously inactive account, which is recently credited at a considerable value from abroad (Annex 1, Section 6, point 3n).
- Accounts are opened on behalf of other natural or legal persons and do not show normal and on-going activity with the economic profile and transactions profile of the account, but are exclusively used for the transfer of funds abroad (Annex 1, Section 6, point 5b).
- On-going funds transfers for large amounts from/to low tax countries and which do not implement or partially implement the respective international standards related to the secrecy or from/to high-risk territories, without a clear business purpose related to the economic activity and customer's transactions profile (Annex 1, Section 6, point 5c).
- Funds' transfers from abroad to a customer in Albania, who continuously transfers funds to a third party (Annex 1, Section 6, point 5k).
- Considerable transfers of values arrived from abroad by a natural or legal person without any obvious economic reason (Annex 1, Section 6, point 5o).
- Relationships established to carry out transactions within a short time, which afterwards are terminated (Annex 1, Section 6, point 6d).
- Large amount withdrawals in cash, excluding the cases when the customer specifies particular need for this purpose (Annex 1, Section 6, point 7c).
- Considerable payments in cash for credit cards, particularly if the customer has carried out frequent or large-amount withdrawals (Annex 1, Section 6, point 7g).
- Frequent cash deposits accompanied by withdrawals at ATM or POS particularly if carried out in the same day (Annex 1, Section 6, point 7h).
- Frequent transactions for amounts slightly below the allowed limits for reporting, particularly related to cash or which are carried out at different branches (Annex 1, Section 6, point 7j).
- Use of payments instruments (debit cards, credit cards, pre-paid cards, e-money, in physical and virtual forms), whose procedures, repetition or economic importance is not in compliance with the financial activity of customers or with the distributors or traders' business (Annex 1, Section 6, point 7n).
- Frequent use of large amount of money, of payment services for the purposes of collection or transfer of money, in cases it is noted that transactions do not comply with the economic situation of the customer and which are not completely justified (Annex 1, Section 6, point 7t).
- Transfers or repeated withdrawals of the considerable amounts of money by a customer at a short time (Annex 1, Section 6, point 7u).
- Transfers or repeated withdrawals of considerable amounts of money from and to different counterparties that are abroad, particularly if these countries are not the country of origin of the customer (Annex 1, Section 6, point 7v).
- Large amounts of incoming funds, particularly from abroad, through the accounts that are used less and which are followed by large withdrawals or transfers through producers or to destinations or recipients who are not related to the customer activity (Annex 1, Section 6, point 7dd).
- A bank account held by a natural or legal person is debited or credited at large amounts, which do not justify the economic profile of the customer's transactions (Annex 1, Section 6, point 8d).
- Accounts closed within a short time from their opening, particularly after the bank requests for the submission of the necessary documents, and in the event when respective funds are transferred (Annex 1, Section 6, point 9c).

- A customer shows considerable high profits deriving from fortune games or bets (Annex 1, Section 6, point 9i).
- Frequent transfer of funds at an account held by an individual with low income (Annex 1, Section 6, point 9l).
- A customer carries out transactions at high value by using a pre-paid card, taking advantage by the possibility of filling the card without the physical presence at the bank, through ATMs, internet banking etc. (Annex 1, Section 6, point 16a).
- A customer purchases a considerable number of pre-paid cards issued by the same financial institution (Annex 1, Section 6, point 16b).
- Large balances of debit and credit cards are settled in cash, without any information on the source of funds (Annex 1, Section 6, point 16c).
- A customer credits his account at large amounts almost exclusively, through an ATM, maybe by denoting the purpose to avoid personal appearance at the financial institution (Annex 1, Section 6, point 16d).

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

- The customer resides or carries out transactions with parties, which are located at high-risk rate territories or places and conduct large transactions by unusual procedures, without substantial justifications (Section 6, point 1m) of Annex 1).
- Transactions are not in compliance with the instruments used in the economic activity and the economic or financial profile or in case of legal persons or group, these transactions are not justified properly by the customer (Annex 1, Section 6, point 2h).
- Frequent and large-amount transactions by customers on behalf or in favour of third persons, or by third persons on behalf or in favour of a customer, when the personal, trading or financial relationships between parties are inexplicable, particularly if these transactions seem to be established to not simulate a relationship to other transactions (Annex 1, Section 6, point 2l).

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, GDPML 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' reporting obligations and GDPML's and other competent authorities' tasks and powers.

- The AML/CFT Law should require the competent authorities[17] to establish guidelines, which will assist obliged entities in detecting and reporting suspicious transactions.[18] The guidelines should include the indicators for suspicious transactions that will cover all obliged entities, including DNFBPs. In the development of these indicators all competent authorities, including the specialised law enforcement authorities, should be involved.
- GDPML and competent law enforcement authorities should provide more active feedback on AML/CFT reporting and AML/CFT prevention measures when new technologies and services are deployed.
- GDPML powers to suspend a suspicious transaction (point (g) of Article 22 of the AML/CFT Law), to order the monitoring of bank transactions (point (l) of Article 22 of the AML/CFT Law), to request data from the obliged entities (point (c) of Article 22 of the AML/CFT Law), and to send their reports with the analysis to the General Prosecutor's Office and other competent law enforcement authorities (point (e) of Article 22 of the AML/CFT Law) should be extended to cover also situations, where GDPML suspects that an online fraud or another criminal offence has been committed, or attempted, with no suspicion of money laundering or terrorist financing whatsoever.
- GDPML, 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 the prevention and detection of online frauds and money laundering that the competent authorities may wish to consider including in the list of indicators for suspicious transactions. In this regard, the BoA and/or other competent authorities may use the existing structure of suspicious indicators[19] (e.g., a division per customer/transactions/means and procedures for payments/products, etc.) or include an additional section with indicators that will only target the online fraud, other cybercrime offences and related money laundering.

General indicators:

- 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.

[17] In other countries, for example, the competent authorities for issuing the guidance and indicators include the Ministry (Minister) of Finance, FIU, and/or other competent AML/CFT supervisory/ regulatory bodies.
[18] This is also required by the FATF Recommendation 34.
[19] As provided in the BoA Regulation 44.

Indicators related to bank accounts:

- The client receives a payment via Internet based payment services (e.g. PayPal, Payoneer card) that does not include details of the sender or purpose of the transaction.
- The client sends a request for payment late on Friday afternoon for transfers to customers in countries in a time zone where there are still several hours of banking available.
- The client makes withdrawals of funds received from a foreign jurisdiction where the transfer was made near to the close of business in the foreign jurisdiction and the withdrawals are made after close of business, particularly after close of business on Friday, in the foreign jurisdiction.
- Significant language errors or unusual content are identified in e-mail or fax communication between the bank and its client or in the documents presented to the bank by its client.
- The client ordering a payment to be made to a beneficiary only communicates with the beneficiary via e-mail.
- Funds for goods/services are refunded onto a credit card other than the one used to make the original purchase.
- The total turnover of the account changes suddenly and significantly as compared to the account's long-term average.

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, 13 March 2017, Tirana, Albania: https://rm.coe.int/1680704db8
B. Cybercrime country profile – Albania (Version of 1 March 2017)
C. Law No. 9917 on the Prevention of Money Laundering and Financing of Terrorism, as amended by Law No. 10391, dated 3 March 2011, and Law No. 66/2012, dated 7 June 2012, on some Additions and Amendments to Law No. 9917: http://www1.fint.gov.al/images/Law_no.9917_amended.pdf
D. GDPML’s Letter to the banks, dated 10 May 2016:

Unofficial translation

REPUBLIC OF ALBANIA
MINISTRY OF FINANCE
GENERAL MONEY LAUNDERING PREVENTION DIRECTORATE

Address: "Dëshmorët e Kombit" Boulevard, No. 3, Tirana www.fint.gov.al
Tel/Fax: +355 42 24 46 02

Protocol No. 332. **Tirana, on 10.5.2016**

Subject: *Regarding some cases of fraud and their handling method*

Addressed to: ALPHA BANK
AMERICAN BANK FOR INVESTMENTS
CREDINS BANK
INTESA SAN PAOLO BANK IN ALBANIA
NATIONAL BANK OF GREECE
NATIONAL TRADING BANK
INTERNATIONAL TRADING BANK
PROCREDIT BANK
RAIFFEISEN BANK
THE UNITED BANK OF ALBANIA
THE CREDIT BANK OF ALBANIA
THE FIRST INVESTMENT BANK IN ALBANIA
SOCIETE GENERALE BANK IN ALBANIA

TIRANA BANK
UNION BANK
VENETO BANK

For information: THE BANK OF ALBANIA

TIRANA

Dear all,

In implementing the duties foreseen with Law no. 9917, dated 19.05.2008 "*On the Prevention of Money Laundering and Terrorist Funding*" as amended, we shared with you the typologies and concerns related to different problems, we organized and attended meetings, etc, which had an impact on the continuous improvement of the prevention system in the country, for which, the banking system has indisputable merit, because in spite of all the difficulties, it was still the engine pushing forward and served as a promoter for other entities and actors.

In this context, further in the text we will share with you our next concern related to bank obligations and GMLPD. We have recently been made aware by respective structures of an increase in a typology of fraud and that it is mostly

- hacking of the electronic communication established with some customers (via e-mail, cell phone, etc.) by unknown individuals;
- in which case they communicate that there has been a change to the IBAN/No. Of the account abroad where transfers must be made (for respective reasons);

actions that result with the customer's trust and consequently their request for conducting the transfer abroad and its processing by the bank, only for the customers to later realize that the whole scheme was just a fraud.

Such schemes have affected a category of individuals and businesses, defrauding and depriving them also of very high amounts.

The aforementioned typology, in general, was not reported as RAD by the banks because it appears that they believed the issue to be complete by having it sent to the Police/Prosecution or by the customers raising charges themselves, but that is not the case, for the following reason:

➢ Law No. 9917 dated 19.05.2008, as amended,

a) in Article 1 foresees that "***The purpose of this law is to prevent*** the laundering of money and other ***products derived from acts of crime***, as well as the prevention of funding for terrorism";
b) in Article 12 (**Reporting before the responsible authority**) items 1 and 2, among other things, it foresees that "

1. Entities shall submit a report to the responsible authority, where they present their suspicions regarding cases where they know or suspect that there is in fact, or that there is an attempt at laundering of products gained from criminal offenses, terrorist funding ***or that the funds involved result from criminal activity***. *Reporting shall take place immediately and no later than 72 hours.*
2. *When an entity which is asked by a customer to carry out a transaction has doubts that the* ***transaction may involve*** *the laundering of products derived from crime, terrorist funding* ***or funds that result from criminal activity,*** *it should not carry out the transaction but report the case immediately to the responsible authority and seek guidance on whether or not to carry out the transaction (.......)*

forecasts, which unequivocally compel banks to report any case linked to a criminal offense, from which criminal activity could derive.

- The execution of transactions for clients, irrespective of their request (they could have fallen prey to fraud), based on the forecasts for the necessary/extended vigilance, can frequently be detected as an anomaly from the very onset of transfer processing procedures as they might not be in accordance with the customer's regular activity, the nature of transfers they carry out as well as be noted from the type of questions addressed to the customer, etc. Hence, the detection of such cases of fraud also comes as a result of the application of measures as foreseen with Law No. 9917, dated 19.05.2008, as amended

- If the GMLPD is informed on time, in principle it would be possible, through cooperation with our counterparts abroad, to make it possible to block funds abroad and start respective criminal procedures against the suspects, as well as administrative procedures for returning the amounts taken to the persons defrauded

- By informing the GMLPD regarding the diversity of such frauds, the way it is carried out, the area where it occurs, the category of customers affected, the countries where the funds are transferred to, etc., in principle, it would be possible for them, in cooperation with the Police and/or Prosecution, to find real criminal networks and not just deal with one isolated case at a time.
- Cybercrime is the next challenge that the prevention system will have to confront since the abuse of the banking system by criminal individuals/groups has a negative effect in the assessment of the effectiveness of the local system to cope in this respect (which is not a duty of the DPPPP)

Therefore, in line with what was said above, we beseech and request

- A summarized report on such frauds for the time period starting from 2014 onwards
- That you adapt to this request and the approach explained, so that such reports are sent continuously and as quickly as possible after the moment of detection.

You are kindly asked to provide the information, in full and correct, to the General Money Laundering Prevention Directorate by **27.05.2016**

Thanking you for your cooperation,

Agim ISMAIL

__

DIRECTOR OF THE STRATEGIC AND OPERATIONAL ANALYSIS DIRECTORATE