Money laundering patterns in Eastern Europe

Policy recommendations based on investigative journalism

AUTHORS:

Attila Biro, RISE Project Romania

Elena Calistru, Funky Citizens

Iurie Sanduta, RISE Moldova

February 2018

This document is published in the project „Money laundering patterns in Eastern Europe" implemented by RISE Moldova and RISE Project (Romania) with the help of a grant offered by The Embassy of Netherlands in Romania, within the MATRA Program. The opinions and findings are of the authors and do not necessarily reflect the opinion of the donor.

1. CONTEXT

The case for looking at the use of cybercurrencies in criminal activities related to money laundering

Current developments related to the rise and fall of Bitcoin have boosted the already strong debate about the increased presence of cryptocurrencies (and the broader world of blockchain) in the global financial flows. Whether or not it is a speculative bubble, we should consider the existing evidence that the criminal enterprise was and still is largely responsible for the value of Bitcoin and for the increased demand for other alternative cryptocurrencies.

Whilst global law enforcement cases show that some agencies get better at identifying the patterns in using cryptocurrencies in the criminal activities, they also show that this leads to criminals trying to use even more innovations and alternative anonymous cybercurrencies to escape the effects of investigations. The continuous developments in this area also show that law enforcement needs its own efforts and resources to keep the pace with technological innovation particularly when it comes to identifying the increasingly sophisticated money laundering patterns resulting from the use of these new tools.

Is there a case for a cybercurrency-focused view on criminal activities in SEE?

Eastern-European countries like Romania, Bulgaria, Republic of Moldova or Hungary are harbors for money laundering operations. Money laundering is the tool that connects organized crime and white-collar crime networks. Small networks of organized crimes to transnational networks use money laundering schemes to launder their earnings from criminal activities as drug trafficking, human trafficking or corruption. These activities usually happen through vast networks that sometimes cover several countries.

One of the best examples is “The Russian Laundromat”. A complex system for laundering more than $20 billion in Russian money stolen from the government by corrupt politicians or earned through organized crime activity. It was designed to not only move money from Russian shell companies into EU banks through Latvia, it had the added feature of getting corrupt or uncaring judges in Moldova to legitimize the funds. This was one of the investigation done by Organized Crime and Corruption Reporting Project- the umbrella organization for Rise Project, Rise Moldova, Bivol - Bulgaria and Atlatzo- Hungary.

Our investigations show that criminal organization operate now in cyberspace. Using new technologies, the products of criminal operations are laundered. The dark web is also used by the organized crime for all sorts of criminal activities. There are some investigations done by the authorities, but few of them focus on identifying the patterns that might lead to better law enforcement policies or procedures to mitigate them.

We have applied the tools of investigative journalism to determine the patterns of the usage of cryptocurrencies based criminal operations in Romania and Republic of Moldova. Our findings

offer arguments for identifying the policy recommendations that might provide a law enforcement answer to them by looking at:

- the new types of money laundering cases occurring using new technologies and possible patterns
- the vulnerabilities of the law enforcement and justice systems to this kind of illegal activities
- the legislation, institutional capacities and transparency in the financial and public sector in each country.

2. STATE OF PLAY

Even if it is almost impossible to have a full picture of the scale of crimes involving cybercurrencies (whether they facilitate crime or crimes are a side-effect of their increased usage), global law enforcement recognizes that cryptocurrency can become a criminal's playground. This is true for at least several major areas: tax evasion, corruption, smuggling, extortion, human and drug trafficking. Money laundering crimes become of particular importance in this regard because these types of predicate offenses generating illicit proceeds can benefit from the challenge of anonymity provided by cryptocurrencies.

Our focus was on two countries in which are particularly vulnerable to money laundering for these crimes – Romania, an EU member state at the border of the Union, and Republic of Moldova, a non-EU state but which is at the very border of the Union. Both countries are members of the Council of Europe and need to comply with Financial Action Task Force (FATF) recommendations, the framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

Both countries have Financial Intelligence Units (FIU) that stand at the core of institutional efforts to fight money laundering, but the models are quite different. The law enforcement structures in the two countries also have some significant differences, but they are comparable. From this point of view, we believe that an analysis of the legal and institutional framework in the two countries can provide valuable insights on the effectiveness and vulnerabilities of these systems in dealing with transnational and cross-border challenges. In an area of continuous technological innovation that often offers a time-advantage to the criminals, the authorities need to adapt to the swift changes whilst also fighting the administrative inertia or bureaucratic tempo that might act as a deterrent to fighting effectively with money laundering.

Romania

Main piece of legislation:
Law no. 656/2002 on the prevention and sanctioning of money laundering, as well as for setting up some measures for prevention and combating of terrorism financing acts, republished;

Institutional framework – administrative model for FIU
National Office for Prevention and Control of Money Laundering (NOPCML) - managed by a President, appointed by the Government, among the Members of the Board of the Office, who acts also as credit release Authority.

The Office's Board is the deliberative and decisional structure, being made of one representative of each of the following institutions: the Ministry of Administration and Interior, the Ministry of Public Finance, the Ministry of Justice, the General Prosecutor's Office by the High Court of Cassation and Justice, the National Bank of Romania, the Court of Accounts and the Financial Supervisory Authority, appointed for a five-year period, by Government decision. Since 2017, the deliberative and decisional activity no longer refers to the specific cases analyzed by the Office's Board, but it is mostly of a strategic nature. Its main attributions consist in:

- Receiving, analyzing and processing financial information and sending over to law enforcement authorities the suspect cases
- Supervision, verification and control of the reporting entities which are not, according to the law, under the prudential supervision of other authority.
- The Office's function as responsible factor in the international sanctions regime
- The prevention and combating terrorism financing acts.
- Receiving, processing and analyzing requests of information.
- The Office's cooperation with national and international authorities
- The management of human, financial and accountancy resources and realization of internal public audit.

Compliance with international standards

- FATF recommendations and EU Directives are mandatory
- member of Egmont Group since May 2000
- member of the FIU.NET network in 2004

Republic of Moldova

Main piece of legislation:
Law no. 190-XVI of 26.07.07 on preventing and combating money laundering and terrorist financing

Institutional framework – prosecutorial model for FIU

The Service for Prevention and Combating Money Laundering (SPCML) - operates as a specialized body assigned the status of independent subdivision within the National Anticorruption Centre, established on 15 September 2003. The SPCML basic functions, as in accordance with Law 190-XVI of 26.07.2007 "on preventing and combating money laundering and financing of terrorism" consists in receiving, processing, analyzing and disseminating the information received from non-banking financial institutions and banks, including specialized professions. Its main attributions consist in:

- Receiving, analyzing and processing financial information and further submitting the data to law enforcement agencies and other institutions
- Prevention measures also reflected in the annual action plans on the implementation of the National Strategy for prevention and combating money laundering and terrorism financing

- Cooperation with the specialized authorities at the national level, including the Ministry of Internal Affairs, the Intelligence and Security Service, the Prosecutor General, the State Tax Service, supervision bodies, and reporting entities.

Compliance with international standards

- FATF recommendations and EU Directives are binding (Association Agreement the Republic of Moldova – EU)
- member of Egmont Group since May 2008

3. CHALLENGES & OPPORTUNITIES

The new European legislation and standards

On 26 June 2017, the Fourth Anti-Money Laundering Directive entered into force. It strengthened the existing rules and aimed at making the fight against money laundering and terrorism financing more effective.

In June 2016, the European Commission published the proposal to amend the fourth anti-money laundering directive (2015/849). The European Council and the European Parliament reached a political agreement in December 2017 on the content of the proposal. They will now be called on to adopt the proposed directive at first reading. Amongst other measures, the proposals require platforms that transfer bitcoin and "wallet" providers that hold cryptocurrencies for clients to identify users. The new rules also aim to:

- prevent the use of the financial system for the funding of criminal activities
- strengthen transparency rules to prevent the large-scale concealment of funds
- improve transparency in the ownership of companies and trusts
- strengthen checks on risky third countries
- address risks linked to prepaid cards and virtual currencies
- enhance cooperation between the national financial intelligence units

The FATF recommendations implementation

Romania's 4th round Mutual Evaluation Report relating to the implementation of anti-money laundering and counter-terrorist financing standards (MER) was adopted in April 2014. Two years later, in April 2016, the country presented a first interim report under the regular follow-up process. The Secretariat noted that, although a number of legislative remedial actions had been prepared, limited concrete progress had been achieved.

At the June 2017 Plenary, the Secretariat noted that three key legislative processes were still underway: amendments to the AML/CFT Law aimed at addressing major deficiencies under R.26; a new AML/CFT intended to transpose the 4th EU AML Directive into national legislation; and amendments to the Emergency Ordinance on the implementation of international sanctions.

Since none of those draft pieces of legislation were in force by the time it prepared its analysis, the Secretariat was not in a position to conduct a detailed evaluation of progress reported by Romania. However, it noted that the envisaged changes could address a number of significant gaps identified under the core and key Recommendations in the MER. During the Plenary meeting, Romania informed the Secretariat that the amendments to the AML/CFT law had been promulgated by the President of the Republic on 31 May.

Considering the expected timeframe for the adoption of the other two pieces of legislation (i.e. by the end July regarding the new AML/CFT law; by end of year regarding the amendments to the Emergency Ordinance), the Plenary asked Romania to report back at the 56th Plenary in April 2018, with a view to applying for exit from follow-up on that occasion. This would be in line with the four-year deadline for exit from follow-up set by the revised Rule 13 of MONEYVAL's 4th round rules of procedure.

The last Mutual Evaluation Report relating to the implementation of anti-money laundering and counter-terrorist financing standards in Moldova was undertaken by the Financial Action Task Force (FATF) in 2012. According to that Evaluation, Moldova was deemed Compliant for 4 and Largely Compliant for 18 of the FATF 40 + 9 Recommendations. It was Partially Compliant or Non-Compliant for 3 of the 6 Core Recommendations.

US Department of State Money Laundering assessment (INCSR)

Both Romania and Moldova were evaluated as "Jurisdiction of Concern" by the US Department of State 2016 International Narcotics Control Strategy Report (INCSR). Key Findings show that:

"**Romania**'s geographical location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons by transnational organized criminal groups. As a result, Romania is vulnerable to financial activities associated with such crimes, including money laundering. […] Though Romania is not a major financial hub and its exposure to foreign proceeds of crime may be limited, there are nevertheless indicators suggesting that organized criminal groups from the neighboring countries and Italy invest in Romanian assets. Romanian organized criminal groups participate in a wide range of criminal activities in Europe, including prostitution, cigarette smuggling, extortion, and trafficking in narcotics, and have collaborated to establish international criminal networks for internet fraud activities and related money laundering schemes. Romania has some of the highest rates of cybercrime and online credit card fraud in the world. Studies have found Romanian servers to be the second largest source of cybercrime transactions worldwide. Although a majority of their victims reside in the United States, Romanian cybercriminals are increasingly targeting victims elsewhere in Europe as well as in Romania itself."

"**Moldova** is not a regional financial center. The economy is largely cash-based and remains highly vulnerable to money laundering activities. The Government of Moldova monitors money flows throughout the country, but does not exercise control over the breakaway region of Transnistria. Transnistrian authorities do not adhere to Moldovan financial controls and maintain a banking system independent of, and not licensed by, the National Bank of Moldova (NBM). The breakaway region of Transnistria is highly susceptible to money laundering schemes. […] Criminal proceeds laundered in Moldova derive substantially from tax evasion,

contraband smuggling, fraud, and corruption. Money laundering occurs within the banking system, exchange houses, and the offshore financial centers in Transnistria. Currently, 11 banks are operating in Moldova. Neither offshore banks nor shell companies are permitted; despite this ban, shell companies continue to be used to launder illicit proceeds. Internet gaming sites exist, although no statistics are available on the number of sites in operation. Internet gaming comes under the same set of regulations as domestic casinos. Enforcement of the regulations is sporadic."

On the ground journalistic investigations

We have indexed until December 2017 - 12 cases sent to trial in Romania related to cryptocurrencies use in criminal deals. In 11 of them cryptocurrencies where used to pay drugs. The buy was set up on darknet so tracking down the buyer and seller would be almost impossible. Interpol experts contacted by RISE Project confirmed the fact that at this time Bitcoin is used mostly in drug related transactions.

In October 2017 The Bucharest Court of Appeal has sentenced AL. M.K. to 4 years and 9 month detention for drug use and international high-risk drug trafficking. On 02 February 2017 a package arrived at a DHL delivery point in Bucharest. Al. M. K. immediately came to pick it up. Because he couldn't show an ID, the DHL employees didn't handed him the parcel. The next day the pack was retained by prosecutors with an warrant issue. The 5.6 kilos weight delivery was dispatched by ADP - Logistics Holland, containing different types of drugs, mostly hallucinogenic mushrooms and psychedelic plants. Al. M. K was caught red-handed by Officers from the Romanian Anti drug Brigade (BCCO) when he signed for the delivery and received the package. BCCO also searched the address and found other quantities of drugs. Al. M. K bought the drugs from Holland using the website www.avalonmagicplants.com. He said the drugs were for personal use and that he payed 200 euros for the products using Bitcoin.

In June 2016 the Romanian authorities received extradition request from Denver Office of U.S. Immigration and Customs Enforcement for Filip Lucian Simion (32), Romanian citizen. He supposedly led a criminal group named "ItalianMafiaBrussels" or " IBM" indicted for importing controlled substances and money laundering. IBM operated online as a Darknet vendor, using encrypted email and TOR-based online black markets, to sell MDMA to U.S. and Canadian customers. The payment for this drugs could be made only in bitcoin. F.L.S. taught his clients to pay from different addresses, using specific techniques in other to mask the transactions. He also payed the other defendants from Romania and Belgium for obtaining, preparing, packing and delivering the merchandise to US.

The group operated from January 2013 to May 2016, when a joint U.S.-European law enforcement action dismantled the ItalianMafiaBrussels Drug Trafficking Organization. 10 defendants have been arrested in Bruges, Belgium, and surrounding areas.The extradited defendants, Filip Lucian Simion and Leonardo Cristea, were arrested simultaneously in Bucharest, Romania. They face a maximum possible penalty of 20 years' imprisonment.

19 May 2017 with The Southeast European Law Enforcement Center support, the Bulgarian authorities announced the seizure of 213,519 bitcoins. The cryptocurrency was the alleged product of transnational cybercrime operations. The data released by SELEC shows that a

criminal organized group of Bulgarian nationals targeted the critical cyber-systems in Macedonia, Hellenic Republic, Romania and Republic of Serbia. The modus operandi used was the following:

- First step was to recruit Customs officers, who the would deploy a a virus in the Customs' informatic systems.
- The virus would permit remote access to the customs database.
- Once in the system the perpetrators modified the internal documents for cargo transports so appeared that the cargo was already checked and passed. In reality the merchandise was not verified.

Sources explained that for each truck the Bulgarian network would be paid up to 25.000 euro in bitcoins.
The seizure of the bitcoin is a matter of controversy. The Bulgarian authorities denied publicly that they actually did froze the 213.519 bitcoins. On the other hand SELEC maintains the position that the investigation was carried out and the cryptocurrency seized.

***

OneCoin is an invented virtual currency and has no real support. From a legal point of view, it is not registered with any accredited entity and is not recognized by any competent forum. The site https://coinmarketcap.com/ is the one that offers the best information about virtual coins that exist on the market. About OneCoin does not show any information. In fact, OneCoin is an MLM business. The mother company is called One Life and claims to have over 3 million members. The currency is not tradable and their clients can not withdraw their investment. The only option they have is to buy surplus products on a site owned by a company which has its headquarters in Umm Al Quwain - Free Trade Zone Authority. Any litigation is settled at the London Arbitration Court.

When you get into the OneCoin business you buy an educational package. If you want to start earning, you have to bring other people. Which, in turn, to invest. And you are given a percentage of what they invest. You can not withdraw the investment, you can not change the currency, the money is blocked.

OneCoin was brought to Romania in 2015 by a former salesman of thermopanes - Cristi Calina. The promoter of the virtual coin is Ruja Ignatova, a Bulgarian citizen, convicted for fraud in countless countries. Two years after its launch on the Romanian market, One Coin Romania went into sight of anti-fraud inspectors. This has happened because National Agency for Fiscal Administration have been received several complaints regarding possible fraud and tax evasion in the OneCoin business.

In Hungary, the Central Bank warned the population that OneCoin is a pyramid scheme. In Germany, the Federal Financial Services Authority - BaFin - has frozen the accounts of OneCoin. Thus, 29 million euros were blocked from any kind of transaction in order to be returned to investors. In Colombia, USA, Italy – OneCoin was banned.

4. CONCLUSIONS AND RECOMMENDATIONS

The results of the investigative journalism effort show that the use of cryptocurrencies is not yet identified by national authorities in the two countries as a priority for their anti-money laundering legislative and institutional framework. The answers of some authorities show that most of them do not consider it a strong threat but do expect to mitigate the risks associated with cryptocurrencies through EU framework.

For money laundering, the entire purpose of the criminal activity is to separate the perpetrator's identity from financial transactions. AML efforts should therefore look at cryptocurrencies especially when efforts to meet international standards are underway and cybercrime is prevalent in your country.

However, what the investigated cases underline is a fact well-known - Bitcoin itself is not truly anonymous because the entire history of transactions is visible to all users. On the other hand, criminals are also aware of this fact and they are increasingly "investing" in anonymous cryptocurrency variants known as 'altcoins.'

However, regardless of the level of technical anonymity, one fact gives law enforcement an advantage: criminals must eventually exchange their crypto-currency for fiat currency at some point. But even this angle offers AML authorities two possible choices which engage different resources – to follow the deanonymization or to detect anomalies in transactions. In doing so, authorities can use or be aware of the same techniques to track and monitor transactions (blockchain can also be used to monitor complex transactions).

The new proposed EU agreement on amending the 4th AML Directive also targets exchange platforms for bitcoin and other virtual currencies in the effort to prevent terrorist financing and money laundering. In this context, we believe that the cases identified in the SEE region might provide valuable insight for the amendment of the EU legal framework. Even though the volume of cases in this area is rather small and often related to minor value criminal offences, they can offer a good overview of the challenges AML authorities can face when dealing with innovative ways of laundering the proceedings of crimes.

Opportunities for action

- Romania has not yet even started the process to transpose the 4th EU AML Directive and an infringement procedure is underway.
- Moldova also needs to align its legislation to the EU Directives, due to the Association Agreement.
- Both countries need to comply with the FATF recommendations which are not yet fully implemented
- Romania does not yet have a comprehensive strategy for fighting money laundering (NOPCML only adopted an Operational Strategy 2017-2020 which is solely focused on the institutional actions to be considered in the respective timeframe) and did not conduct a national risk assessment analysis (even though it is a FATF recommendation)

- Moldova adopted in 2017 a Report on National Money Laundering and Terrorist Financing Risk Assessment and an Action Plan to mitigate them
- There is a significant space for improvement both at legal and institutional level and the opportunity given by the need to comply with the EU legislation and the FATF recommendations can be used in order to provide comprehensive and integrated solutions for AML

Recommendations

- ❖ Improve and refine the legal framework, policies and strategies with a view of including the EU and international efforts in the area of AML and the FATF recommendations (an effort that should include risk and impact assessment). While a sense of urgency might dominate the need for legislative intervention, the quality of such legislation should be the primary concern.
- ❖ Evaluate and improve the institutional framework and the cooperation between all the stakeholders relevant for the AML efforts. No matter the preferred model for FIU (administrative, law enforcement, hybrid), the cooperation effort should be inclusive, based on a common vocabulary and commitment and sufficiently agile to adapt to the increasingly sophisticated models used in criminal behavior associated with money laundering.
- ❖ Sufficient technical, financial and human capacity for the Financial Intelligence Units, law enforcement professionals and the judiciary in the field of financial investigations and recovery of illicit proceedings is mandatory. The level of sophistication in criminal behavior and the risks of a EU-border environment should be mitigated with adequate resources.
- ❖ Transnational but also interinstitutional cooperation should have at its base not only a viable data and information exchange mechanism but also a data-driven approach in prevention and in the identification of patterns that might appear.
- ❖ The innovations in the criminal enterprises and the vulnerability of the two economies to cybercrime should be considered. A particular area of interest should be to map the most vulnerable sectors as well as the emerging trends related to the use of cryptocurrencies in money-laundering related to offences such as drug and human trafficking, corruption, smuggling.