MONEY LAUNDERING AND VIRTUAL FINANCIAL RESOURCES

MOMČILO SEKULIĆ[1], ANA MATOVIĆ[2] & DJORDJE MILOŠEVIĆ[3]

[1]Faculty of Law, Megatrend University, Belgrade, Serbia, e-mail: momo.sekulic@t-com.me.
[2]Faculty of business studies and law, Belgrade, Serbia.
[3]University of Criminal Investigation and Police Studies, e-mail: djodjolos@gmail.com.

Abstract Money laundering is a complex phenomenon that represents the direct impact of organized criminal groups on legal financial flows. As a particularly dangerous dimension of illegal activities, the author emphasizes the possibility of masking them through the investment of illegally acquired funds in legal public or private affairs. The author analyzes the structure of this illegal activity, showing its adaptation to modern communication conditions, which is why he notices the importance of evolving this illegal phenomenon in the online environment. The predominant part of this paper is dedicated to the introduction of numerous ways of placing criminal profit in the regular monetary market through the information and communication benefits of the Internet. In his research, the author does not stay within the framework of the visible part of the web. His special attention is focused on the high-tech circumstances and communication capacities of the dark web, in order to emphasize the inexhaustible possibilities of hiding, "laundering" and further placing "laundered" money that originates from criminal activities.

Keywords: money laundering, online environment, internet, finanscial crime, dark web.

University of Maribor Press

DOI https://doi.org/10.18690/978-961-286-442-2.65
ISBN 978-961-286-442-2

1 Introduction

By its nature, money laundering is an illegal activity carried out by individual or group carriers of criminal activities, which occurs outside the usual range of economic and financial statistics. As money laundering is a consequence of almost all kinds of profits, it can be done anywhere in the world. In general, money launderers tend to seek countries or monetary markets where there is a low risk of detection due to security-porous regulatory systems or inefficient law enforcement agencies. [Washington, D. C., 2020].

Modern information technology is a reality in all its existing forms. Internet payments, electronic money and digital money, internet of networked electronic items and market information systems are an integral part of financial flows. Mobile payments are a great promise in terms of modernizing the method of payment, but they can also be a problem of preserving the payment integrity of legal entities and individuals. Virtual currencies have created a bridge for online financial activities, connecting global web users and accepting cryptocurrency as an alternative to official currencies and securities supported by government systems. It is unlikely that international law or national laws will capture all the changes taking place in the new technology market and adapt to them in real time [Şcheau; Pop Zaharie;2017].

More recently, professional money laundering networks have begun to use virtual finance as a means of transferring, collecting, or hidding in layers the criminal proceeds. The following are typical cases of online money laundering through the manipulation of virtual funds in the specific circumstances of the visible and hidden part of the web. [Paris, 2020].

2 The means of execution

- Multiple instant transfers of large amounts of virtual funds to foreign web service providers

The local provider reported a suspicious transaction involving the purchase of a large amount of virtual assets from various individuals and their subsequent direct transfers to foreign providers. In several different cases, individuals had the same residential address, while most sites with virtual assets were accessed

from the same IP address. This indicates the potential use of money carriers by professional money launderers. In addition, multiple stratification of decree money funds was done before the purchase of virtual funds by money carriers. In order to conceal the origin of the funds, cash was first deposited in various accounts in a number of financial institutions throughout the territory of the same state. These funds were then further transferred to different accounts held in the name of persons who are registered citizens of the same state. Electronic payments were made to accounts in smaller amounts. After that, the funds were transferred to another group of accounts before they reached the accounts of the money carriers, which was done through the services of local providers. The virtual funds were then immediately purchased and transferred to foreign providers. More than 150 individuals were involved in this money laundering case, who were responsible for transferring a total of $ 108,352,900 (the equivalent of 11,960 Bitcoins) to multiple accounts with virtual funds managed by two foreign providers.

- Multiple transfers of various virtual funds to foreign providers

The local provider, which provides virtual asset exchange services, reported that approximately 400 million KRV (about 301,170 EUR) had been stolen from phishing victims. This amount was exchanged for virtual funds, which provided layered concealment of money laundering. What triggered the reporting was to undertake multiple high-value transactions in order to transfer virtual funds to a single crypto wallet with a foreign provider. The stolen funds, denominated in decree currency, were first exchanged for three different types of virtual funds, and then deposited in the suspect's crypto wallet, which is kept with a local provider. The suspect then tried to conceal the source of these funds with new transfers, as many as 55 times, through 48 separate accounts held with various local providers, before transferring them to another virtual wallet housed with a foreign provider.

- The initial deposit does not match the investor profile

The presence of the following suspicious indicators prompted the bank to report an irregular transaction to the competent authorities, which led to an investigation into money laundering: 1. transactions that do not comply with the account holder's profile - in the first two days after opening a personal account

for a young individual deposits of a commercial nature from various legal entities in large amounts; 2. transaction forms - deposited funds are immediately transferred to the accounts of several providers (in one day) for the purchase of Bitcoin; 3. client profile - one of the buyers of virtual assets was already known to the bank in connection with an earlier case of fraud. The bank also provided the competent authorities with IP addresses used for internet banking services. Based on the investigation, it was determined that the owner of the newly opened personal account is a money carrier, when the criminals recruited him on the social media platform in order to help receive requests for payment for goods sold online. However, it was established that such funds were deposited by other damaged companies and that these were not payments for the ordered goods. The deposited funds were immediately transferred from a personal bank account through several split payments to another account with the joint stock company, and were exchanged with virtual money held in several accounts managed by local providers, who were immediately blocked from accessing the newly opened account. In addition to reporting a suspicious transaction, the bank also suspended suspicious transfers, which allowed for subsequent confiscation of funds. The local provider also noticed irregularities in the funds received and provided useful information to assist in the investigation. The information included: the circumstances where the virtual assets were purchased, transactions and customer data, such as the crypto wallet address, a copy of the misused purchase identification document and the name of the alleged buyer, which allowed the authorities to request additional information from banks such as statements from a bank account.

- Transfers recurring in time

A local securities company has filed a report on suspicious transactions due to unauthorized payments with virtual funds, which link the account of their broker with the account of a foreign citizen. The securities firm reported irregular activity after determining that the foreign national intended to make transfers totaling $ 4.8 million, when two separate transactions occurred six minutes apart on the same day, after which it handed over to the broker a request for a trading account relating to its next business day. It has been determined that the crypto wallet is not kept in the Cayman Islands. Reporting on suspicious activity led to a successful exchange of information with foreign financial institutions and a successful return of most of the funds to the victim, because foreign authorities managed to block the suspect's account on the online platform before the criminal money laundering activity ended.

- Using an IP address associated with the AlphaBay marketplace on the dark web

AlphaBay is the largest criminal market of the dark web, which was blocked in 2017, and was used during the two-year period by hundreds of thousands of Internet users to buy and sell illegal drugs, stolen and fake identification documents and access devices, counterfeit goods, malicious viruses and other tools. for hacking computers, weapons and toxic chemicals. The website functioned as a hidden service on the TOR network to conceal the locations of the underlying servers, as well as the identities of its administrators, moderators and users. AlphaBay merchants used a number of different types of virtual assets and had approximately 200,000 users, 40,000 sellers, 250,000 entries, realizing virtual asset transfers of over $ 1 billion. In July 2017, the US authorities, with the help of foreign partners, suspended the servers that maintained activities on the AlphaBay dark web market, during which the administrator was deprived of liberty and physical and virtual assets were confiscated, both those found on the AlphaBay market and those was illicit proceeds of criminal trafficking. Criminal activities in the AlphaBay market were detected by monitoring transactions of virtual funds from this market to other crypto accounts, after which bank accounts with funds controlled by the administrator of the AlhaBay market were discovered. The multi-layered nature of this dark web market was a great cover for money laundering constructions.

- Use of mixing and rotating virtual assets services with the Helix provider

The dark web provider Helix provided, for a fee, over a three-year period, a service of mixing and rotating virtual assets so that users could conceal their source or owners. Helix transferred over 350,000 Bitcoins, the value of which at the time of the transfer was more than $ 300 million. The operator specifically advertised the service of mixing and turning virtual funds as a way in which transactions on the dark web can be concealed from the law. In February 2020, criminal charges were filed against an individual who ran Helix, including those against money laundering and making unauthorized transfers. Helix as a provider was connected to the dark web market AlphaBay, until the closure of this criminal online market.

- Use of a decentralized crypto wallet

This case shows how criminals use a decentralized virtual wallet to cover up the sources of illegal funds generated by illegal drug trafficking activities. In this case, the criminals sold a large amount of narcotics on the Internet and demanded payment not only in decree currency, but also in the form of virtual funds with Bitcoins, EX-codes and EXMO checks. Illegal funds were received in decreed currency and converted into virtual funds with the help of an anonymous account on the blockchain online trading platform. Such virtual funds were converted back into decree currency via a software changer, before being returned to the personal accounts of criminals 'bank cards. As for the illegal proceeds from the sale of narcotics, which were received in the form of virtual funds, it was first transferred to decentralized Bitcoin wallets owned by the same criminal entities, and then further transferred to other Bitcoin wallets located on various dark exchanges. web. This increases the difficulty in detecting and tracking virtual asset flows. In the end, the laundered virtual funds were converted back into decree currency before being paid into the bank card accounts of one particular criminal entity. Consequently, he was sentenced to seven years in prison and an accompanying fine upon completion of the trial.

- The client refuses to provide information on the origin of the funds

The bank reported a suspicious transaction made to the account of a local company, which held funds generated by the sale of coupons to purchase products. In this case, it was bioplastics. The funds were deposited by individuals and legal entities, and some of them were originally in the form of virtual funds. Despite further investigations by the bank, representatives of the account holders did not provide information on the origin of the funds. Subsequent analyzes by the competent authorities showed that the funds sent by the company showed links with entities related to organized crime and other funds obtained from fraudulent construction.

- The client profile does not correspond to regular trading of high amounts of virtual funds

The provider providing online exchange services and the payment company have submitted reports to the competent authorities on suspicious transactions related

to the trade of large sums of virtual funds. The trade started when an account was opened on the online exchange. In particular, the account holder performed various purchase and sale transactions with virtual assets in the amount of over EUR 180,000. This amount did not match the account holder's profile, including his occupation and income criteria. The analysis revealed that virtual funds were subsequently used for: 1. transactions on the darknet market; 2. online betting; 3. transactions with providers that provided online services without adequate money laundering control or were already known to the competent authorities in connection with money laundering of several million US dollars; 4. suspicious activities on online platforms that offered peer-to-peer transactions of virtual assets and 5. services of mixing virtual assets. The account holder has also used a multitude of different online services, such as money transfers, online banking and prepaid cards, to transfer a strictly defined amount of funds from his account within the same time frame. It seems that these virtual funds, which the owner of the account had, were sent from the network of individuals who bought Bitcoins for cash. This network included people from Asia and Europe (including Italy), who bought cryptocurrency through money transfers and online financial services. The mentioned account holder received virtual funds on his prepaid cards from individuals from Africa and the Middle East, who in turn collected funds from fellow citizens residing in Europe and other continents. These funds were then used for cross-border transfers and online gambling, and were withdrawn in cash from a number of ATMs in Italy.

- Victims of online fraud who have been turned into carriers of criminal money

In these investment scams, foreign nationals contacted retirees and mostly seniors by direct phone calls, emails or social media and offered them opportunities to invest in Bitcoin or other types of cryptocurrencies, promising to make huge profits due to the growing popularity of virtual assets. and the growth of their value. The initial investment in small amounts (in many cases no more than € 250) was made from the victim's bank account, credit card or other means into various payment services and then ended up in the hands of criminals. Alternatively, the victims were ordered to exchange decree currency for Bitcoins using a virtual ATM, and then to send the funds to the address specified by the criminals. The victims did not know information technology and generally did

not understand the meaning of virtual resources, which is why it was not clear to them what they were really investing in. Criminal entities also asked victims to install a remote desktop application on their computers so that criminals could, under the pretext of support, directly transfer funds to certain accounts. This endangered the victims' computers, so that criminals could make unauthorized money transfers without the victim being aware of it until she discovered that she was missing money in her account. In some cases, criminals have also fabricated articles claiming that celebrities or wealthy businessmen or journalists promote investing in virtual assets, especially cryptocurrencies, giving victims of fraud a sense of trust and justification for "profitable investments" in the online environment.

- Using shell companies on the Deep Dot web

In May 2019, U.S. authorities seized the DeepDotWeb website, based on a court order. The owners and operators of this website are accused of money laundering activities in connection with millions of US dollars from the refund, which they received for referring individuals to the dark web market from the disputed website. Through referral links, DeepDot web owners and operators received reimbursements, representing commissions on income from the purchase of illegal goods, such as fentanyl and heroin, that individuals sent to the dark web market from the disputed website. These refunds were made in virtual funds and paid into the crypto wallet for Biktoine on the DeepDot web. To disguise and mask the nature and source of the illicit earnings, which amounted to over $ 15 million, DeepDot website owners and operators transferred their illegal refunds from their Bitcoin crypto wallets to other Bitcoin crypto wallets, as well as to bank accounts they controlled in name shell company. Defendants used these affiliates to relocate their unauthorized profits and perform other activities related to the DeepDot web. Over a five-year period, this website received about 8,155 Bitcoins in transfers from the dark web market in the equivalent of approximately $ 8 million. At the time of each transaction, the values of USD and Bitcoin were adjusted. The said cryptocurrency was transferred to the DeepDot web in a virtual wallet, which is controlled by criminals in a series of more than 40,000 repeated deposits, and then transferred to various destinations in over 2,700 transactions. The value of Bitcoin, at the time of withdrawal from the virtual wallet on the DeepDot web, was approximately 15 million USD.

- Using multiple exchanges of virtual funds and false identification documents to register clients on the online stock exchange and obtain prepaid cards

In April 2019, the defendant was sentenced to two years in prison for illegally transferring money after he sold virtual funds (Bitcoins) in the equivalent of hundreds of thousands of US dollars for which he had more than a thousand customers in the United States. Defendant was also ordered to forfeit $ 823,357 in profits. Defendant advertised his services on websites for virtual funds users, personally meeting with some customers from whom he took cash in exchange for virtual funds. Other customers paid for it through state ATMs or money transfer services. The accused received a 5 percent premium for his services at the current exchange rate. He first obtained Bitcoin on an online stock exchange in the United States, but when his activities aroused suspicion and his account was closed, the accused switched to a virtual stock exchange in Asia. Using that online stock exchange, the accused bought Bitcoins in the equivalent of $ 3.29 million. He did this through hundreds of separate transactions, in the period from March 2015 to April 2017. The accused also admitted that he also exchanged his cash in US dollars, which he kept in a neighboring country, for precious metals, and that between the end of 2016 and in early 2018 with other persons brought into the United States an amount of over one million USD in amounts slightly below $ 10,000 to avoid responding to a request for reporting on the origin of the transferred finances.

3 Conclusion

Virtual funds are similar to cryptocurrencies and digital money. They are determined by the anonymity of owners and users, and the lack of regulations to which their use is subject. However, they can be applied in a smaller number of areas on the web, regardless of the benefits of the online environment, compared to virtual and digital money. Internet casinos and online games provide highly developed money laundering schemes. Criminal organizations can exchange virtual funds for the cryptocurrency they will use for the purpose or for online engagement and support of the participant of the game on the web, in order to achieve the best results and collect as many units of these funds as possible [Şcheau; Pop Zaharie, 2017]. Another feature of virtual assets is that they serve as a currency that is exchanged between criminal groups. The value of the action itself may vary depending on the areas of interest of the seller and the buyer. As mentioned, if in the case of virtual money there are algorithms fairly well

established, in the case of virtual funds there is much wider flexibility [Ş cheau; Pop Zaharie, 2017].

Virtual resources and related services on the web have the potential to drive financial innovation and efficiency, but their special features also create new opportunities for money laundering, terrorist financing and other ways in which criminals can launder their income or fund their illegal activities. The ability of a fast cross-border transaction not only allows criminals to digitally acquire, move and store virtual finance, often outside a regulated financial system, but also to conceal their origin or destination and make it almost impossible to detect their suspicious financial activities online. These factors create barriers to the detection and investigation of criminal activities on the public web, and especially in the circumstances of the dark web. [Paris, 2020].

Most of the illegal activities related to virtual financial resources are related to the online activities of financial crime and indicate the existence of money laundering structures. Nevertheless, criminal entities use virtual means to avoid financial sanctions and raise funds to support terrorist organizations, but also to perform other types of illicit acts, such as illegal sale of narcotics and firearms, fraud, tax evasion, high-tech crime (eg cyber attacks resulting in theft), child abuse, human trafficking, and the sale of counterfeit products (very often counterfeit drugs and non-standard orthopedic aids). Among them, the most common type of misuse of virtual funds is associated with illegal drug trafficking, either by selling directly through the exchange of virtual funds, or by using these funds to layer money laundering schemes. The second most common category of their abuse relates to various types of internet fraud and the placement of ransomware.

References

Washington, D. C., Bureau of International Narcotics and Law Enforcement Affairs, United States Department of States. (2020). International Narcotics Control Strategy Report.

Birmingham, Gambling Commission. (2020). The Prevention of Money Laundering and Combating the Financing of Terrorism.

Şcheau, M. C., Pop Zaharie, S. (2017). Methods of Laundering Money Resulted from Cyber-crime. Economic Computation and Economic Cybernetics Studies and Research, 51(3). Str. 299-314.

Bell, A. (2018). Money Laundering in a Digital World. Quantexa, May 1.
Preuzeto sa: https://www.theneweconomy.com/business/money-laundering-in-a
digital-world

Richet, J. L. (2013). Laundering Money Online: a review of cybercriminals' methods. ResearchGate, June 1.
Preuzeto sa: https://www.researchgate.net/publication/257528235

Paris, The Financial Action Task Force. (2020). Money Laundering and Terrorist Financing Red Flag
Indicators Associated with Virtual Assets.

de Koker, L. (2013). The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money
Integrity Risks Within the New Standards Framework. Washington Journal of Law, Technology & Arts,
8(3), Str. 165-196.

Luxembourg, European Parliament. (2020). Improving Anti-Money Laundering Policy: Study for the
Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of
Life Policies.