Social Transformations in Contemporary Society, 2023 (11)
ISSN 2345-0126 (online)

ANTI-MONEY LAUNDERING AND TERRORISM FINANCING ISSUES IN THE PROVISION OF REMOTE FINANCIAL SERVICES

Anastasija Slobodenuka

Mykolas Romeris University, Lithuania/Luxembourg
anastasia.slobodenuk@gmail.com

Abstract

Purpose – to determine and theoretically individualize the modern means of money laundering and terrorist financing using modern technologies, in particular, remotely.

Design/methodology/approach – research is based on the system approach, modern methods of cognition of money laundering in the sphere of remote financial services and features of legalization of these criminal incomes, features of social life phenomena and the accompanying criminal processes that facilitate legalization. Instrumentation to achieve these goals were the methods of criminological and legal research, historical research, system-structural analysis, formal logic, a comparative legal method.

Finding – innovations in financial services, such as new methods of identification, electronic signatures, various platforms for uploading identification and ''know your client'' documents, give fraudsters the opportunity to find new ways to launder money and new opportunities to commit other types of fraud, such as cyberfraud, and identity theft as examples, thus technologies provide new opportunities not only for financial institutions, but for criminals as well.

Research limitations/implications – this analysis will allow to consider the development of trends in a more detailed version, since various external factors have influenced them over the past 5 years. This research will help to predict future trends and develop crisis options in the financial sector and various money laundering prevention methods.

Practical implications – this paper consists of integrated approach to the scientific and theoretical understanding of the problems associated with the manifestations of criminal activity in the laundering of money and terrorism financing in the remote financial sector. The analysis of the reasons for the ineffectiveness of the application of the norms of the current "anti-laundering" legislation and the lack of adequate law enforcement practice.

Originality/Value – The results of the research can be applied in educational and pedagogical activities, in particular, in teaching and studying courses in banking and finance law, in conducting seminars with students of law and economic faculties of higher educational institutions, as well as in conducting research on relevant issues. This research can generate interest in both - the general public, as well as professionals in the field of law, economics, political science and business. Additionally, this research could demonstrate that European institutions initiatives are still having a vague idea of what the consequences might be if new technologies trends are not thought through in advance.

Keywords: anti money laundering; fraud; remote financial services.

Research type: research paper.

ISSN 2345-0126 (online)

Introduction

For a short period of time, money laundering in the sector of remote financial services and terrorism financing has acquired an international dimension and a special danger that poses a real threat to the stability of the financial systems of individual states and the international community as a whole.

At the same time, the degree of importance of the problem lies not only in the volume of financial resources involved in the turnover but also in the actual and potential consequences of their occurrence and circulation.

The rapid development of computer and telecommunications systems in the financial and banking sector led to the appearance of electronic cash and the appearance of a global system of electronic cash settlement, around which a parallel banking system with a whole network of offshore financial institutions was formed. The rapidly evolving new electronic financial infrastructure immediately attracted the attention of criminal communities with its unique capabilities, since it allows you to transfer funds to any country in the world quickly, anonymously, through extremely confusing routes and bypassing state financial control systems. Electronic transfers have been used by criminals as an effective tool that allows easily hide the true sources of cash, launder criminal money and hide your income from taxation.

Currently, technologically advanced countries in the world annually lose billions of dollars due to weak protection of their telecommunications systems. As per Button and Hock (2022) financial institutions always had been the main focus of money laundering.

Moreover, the information space is not only a place, but also a tool for illegal actions on the Internet. Now, to commit a crime in the field of technologies does not even require preparatory "work with the client" and personal contact with the future victim. The above mentioned, significantly complicate the actions of law enforcement agencies in the detection, recording and seizure of forensically important information for further giving it the status of evidence.

Modern technologies in the field of e-commerce also led to the emergence of new means of payments and payments through the global network and its anonymous segments with the help of various crypto-currencies, virtual coins and electronic means of accounting requirements. Unfortunately, the public accessibility of settlement technologies and global distribution has become the reason that these technologies of settlement can be used illegally for the purpose of money laundering via the Internet.

Payments using electronic money usually do not involve documentary confirmation of transactions, nor, as a rule, require careful identification of customers, or openly declare anonymity of payments as the main advantage of using one or another electronic currency in comparison with competing systems. Nowadays, we could see an active proliferation of different e-payment companies, financial companies without "a bank" status et cetera.

Money laundering via the Internet differs from the "traditional" money laundering, where the banking system is used, since internet-laundering is based on the production of various monetary transactions. These can be bank transfers, cash depositing or withdrawal, use of electronic money, money transfer services and other means.

The purpose of this paper is to identify the modern means of money laundering using modern technologies. The research is based on a systematic approach, modern methods of knowledge of crime in the field of the legalization of criminal proceeds. The tools for achieving these goals were the methods of legal research, historical research, system-structural analysis, formal logic, comparative legal method.

The regulatory framework of the study was international conventions, treaties and recommendations of special international organizations, directives and national laws.

ISSN 2345-0126 (online)

This paper is organised in a following manner: the introductory part explains the main issue and the purpose. The first part explains the significance of new technologies in the financial sector and second parts gives a brief overview of identification issues in terms of anti-money laundering. Main results are discussed in the conclusion part.

The significance and ''underwater stones'' of new technologies nowadays

The new technologies revolution has become a global phenomenon as per Puschmann (2017) studies. All over the world, startups offering online payment, foreign exchange, crowdfunding, loan or asset management services have emerged. Polari (2016) has explained this boom as a part of the financial crisis of 2008, two of whose major consequences largely favored the massive emergence of fintechs: the crisis of consumer confidence and the strengthening of financial regulations.

Traditional banks were hit by several new regulations following the credit crisis and also had to deal with the consumer confidence crisis. First, the financial crisis has caused a huge drop in the level of confidence in large banking institutions. While before the banks primary competitive advantage was the image of confidence and solidity that they could offer their customers, it was no longer the case after the crisis, consumers then partly started to distance themselves from these large centralized institutions, to evolve towards a world of connected communities, of which were the few small startups offering financial services at the time. Second, with regard to regulations, the banks had to pay huge fines for non-compliance. In addition, regulators demanded that they maintain a certain level of liquid assets and capital reserves.

These new regulations were intended to minimize the risk-taking of traditional banks, but beyond that also had serious consequences on the activity of them. Most importantly, they had no choice but to pay more attention to their back offices and invest more in compliance and risk management programs. In other words, traditional banks have been forced by new regulations to change their priorities.

It is important to note that this crisis of confidence, as well as the strengthening of financial regulations, were not the only reasons for the success of the financial technology. This success was due to an accumulation of changes in the environment and in the behavior of society, the main elements of which as per Polari (2016) are as follows:

1. The evolution of consumer behavior and preferences: this has played a key role in the evolution of the financial technology because since the development of it, a power transition has taken place between businesses and consumers. Technology has made it possible for these consumers to no longer have to fully comply with the rules of large institutions. On the contrary, it has enabled them to free themselves from these banking institutions by allowing them to seek advice from alternative sources. In this way, consumers have become less dependent and less loyal to these institutions but have also become more demanding in terms of convenience and personalization.
2. The mobile and digital device revolution: over the past decade, the proliferation and widespread adoption of mobile devices has taken place. It also brought with it the revolution in the use of data, powered by social media platforms, as well as new technological infrastructures and developments such as artificial intelligence.
3. The low cost of developing technological platforms: it has never been so easy or so cheap to develop startups in the technological field. Access to open source software and low-cost development tools has greatly encouraged the increase in the number of startups.
4. The increasing speed of change: the adoption of technology is faster, which lowers barriers to entry to the industry and increases competition. Companies with competitive

advantages in these areas must act faster and anticipate to seize the opportunities that arise. This was the case for banks, which in this case were neither fast enough nor innovative enough to anticipate the emergence of fintechs.

5. Profitability of the sector: technology is about to completely transform financial services. It is in fact planned that all financial products, from the most "short-term" like credit cards to the most "long-term" like mortgages, will go digital in the years to come.

The studies of Riemer and Hafermalz found that financial technology try to differentiate themselves from traditional institutions by their unique value proposition, which mainly includes the following:

- Due to their size and youth, financial technologies are receptive to customer needs and therefore adapt their products accordingly. They have the flexibility necessary to guarantee the strategic level of trust, that is to say to pass themselves off as a trusted advisor to customers and ultimately be more customer-oriented.
- They offer fast, online services that are easy to understand. Emphasis is placed on the "user-friendly" character, which is far superior to that of banks.
- Financial technologies use digital technology to offer competitive prices.
- Access to investment opportunities and capital is possible for all socio-economic classes, thanks to crowdfunding in particular. With the banks, the conditions were often complicated to satisfy for part of the population.
- There are many options available to customers, clear benchmarks and the costs of switching from one service to another is low.

However, there are also challenges encountered by financial technologies, and one of them is cyber security. Since the activity of new financial products and services includes the management of extremely sensitive data, it goes without saying that they must be able to protect them against attacks on the internet. According to the studies of Feral-Shuhl (2015) more and more financial data on individuals and companies is available digitally. The risk of breach of the security of this data therefore also becomes higher. The problem is, no matter how much confidence a company may have in the security of its infrastructure, there is almost always a possibility of potential hacking and it is of course needless to say that the slightest flaw in the protection of this data would mean the assured death of a young startup still growing. This is why the issue of cyber security represents a challenge not to be underestimated in the financial technologies sector.

Additionally, it is important to mention that over the past decade, a “shadow economy” has emerged, which provides a market for goods and services for committing cybercrime and for selling stolen goods and information. It means that it provides a “single economic space” for sellers, service providers, fraudsters and customers and allows criminals to organize their activities, according to the studies of Edelbacher and Kratcoski (2012).

This why one of the significant steps forward was that first time cyber-crime was featured in an EU money laundering directive - Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal and included in a list of predicative crimes of money laundering.

Customer identification issues in the provision of remote financial services in terms of anti-money laundering.

Byrnes and Munro (2023) in their studies mention that customer identification in remote financial services is an essential element of collateral combating money laundering and the financing of terrorism, taking into account new specifics of this process. Generally, international anti-money laundering standards are developed by the Financial Action Task Force (FATF),

which issued its first recommendations in 1990 and since then, they have been updated several times. According to the current edition, when implementing such measures, a risk-based approach is mandatory and the basis for this is that the higher the risks are the more stringent measures must be applied to minimize them.

The FATF Recommendations establish only the broadest, most framework requirements for customer identification and also two basic concepts are applied that relate to customer identification and verification - "customer due diligence" and "identification" (Parkman 2020). According to the definitions, a customer due diligence, as a broader concept, includes identification as one of the measures to establish the reliability of information provided by the client for the purpose of anti-money laundering. However, between an ''identification'' and ''due diligence'' there is another definition – ''verification''. Identification is the collection of customer information from a reliable and independent source, and verification is a verification of the data received. When conducting verification in many countries, a conservative approach is used, it means that the collection and verification of information such as date of birth, gender, source of income, registration address, and documents accepted for consideration are limited to the list of official sources of information approved by the state (passport or other identification card).

In the newest Guidance, FATF is trying to define what means ''an official identity'' and came to a conclusion that it ''is the specification of a unique natural person that:

1. is based on characteristics (attributes or identifiers) of the person that establish a person's uniqueness in the population or particular context(s), and

2. is recognized by the state for regulatory and other official purposes.''

There should be a particular proof of identity for financial services, however, it is quite complicate to combine and to put forward the same requirements for different jurisdictions. In a majority of countries, proof of official identity is provided through a document which is usually delivered as a documentation or certification (which could be a birth certificate, an identity card or digital ID credential, passport) that constitutes evidence of core attributes for establishing and verifying official identity.

Here we should remember that we are talking about remote financial services. And in case if these services include a service of legal entities these documents are usually sent by post with apostille or signed by electronical signature and zipped in a file. As the biggest part of remote financial services work with natural persons (for example, pre-paid cards or digital wallets), the type of information could vary, and usually is: ''name, surname, ID document''. Taking into account a nature of these services – all these customers will have common feature – non-face-to-face identification which is always a high risk indicator.

A situation is widespread in the world when the information required to identify a client is unavailable or limited due to a number of reasons and circumstances, for example, when a citizen of another state contacts the bank or the client does not have an identity card.

In his paper, Perlman (2019) mentioned that increased use of electronic identification over physical identification is paving the way for adoption of electronic Know-Your-Customer systems to fulfill customer identification and verification and in order to ensure proper verification in such a situation, in some countries the list of documents that can be used for identification has been legally expanded. Such measures not only ensure compliance with anti-money laundering but also increase the availability of remote financial and banking services. For example, sources of information may include tax information, a work book or records of work in other formats. However, in such cases the risk of fraud is growing rapidly, as a tax information or even an ID document could be stolen and a forgery.

As remote financial services are regarded to be a product of ''new technologies'', hand in hand were distributed new ways of verification. Biometric identification could be done through

technological devices and usually it could be a photo of a client's face, a record of his voice, or an image of a fingerprint. Identification procedures using biometric information require countries to create an adequate and effective infrastructure, including scanners for collecting biometric data, Internet access, a network of agents using certified equipment for collecting and processing data. The advantages are quite substantive - in countries where other mechanisms for identifying clients are not available or not popular, they opt for biometrics. It is caused not by the innovative nature of biometric authentication itself, but by the fact that it is available to any citizen, regardless of the level of literacy and education. The main disadvantage of this method is – its cost, additionally, it requires mass registration of biometric data and their centralized storage. Comparison of fingerprints, a cast of a voice or an iris of the eye is probably a promising technology, but so diverse that it's impossible to determine what will become common practice today.

In world practice, customer identification issues go beyond the scope of the fight against money laundering and terrorist financing. Identification mechanisms directly affect the costs of citizens and private companies, the level of competition in the market. Ultimately, their inefficiency can be a barrier to the receipt of financial services by the population, especially, such services which position itself as ''fast and easy''.

The Fifth EU Directive on Anti-Money Laundering which entered into force in 2018, recognizes the possibility of developing new technologies that can provide safe methods for remote electronic verification of a personality of a customer. While mentioning remote financial services provision, the most popular way of identification and verification will be through a Digital ID system. From FATF Guidance it is clear that Digital ID systems also pose money laundering risks that must be understood and mitigated. It is important to understand that Digital ID systems are representing a bunch of technical challenges and risks, because they often involve identity proofing and authenticating individuals over an open communications network. Consequently, the processes and technologies employed by digital ID systems introduce out of number opportunities for cyberattacks a between the customer and its counterparty. FATF has stated that without assessing of the risk factors money launderers could also abuse digital ID systems by creating false identities.

Increasingly has grown a use of biometric solutions to combat fraud and money laundering. It is noted that in the first place this applies to the Know-Your-Customer tools and online identification. They are relatively inexpensive and still work fast, moreover biometric identification allows you to recognize a person's identity by facial image, fingerprint or voice.

Estonia was one of the first Baltic countries who experienced a biometric solution in their Know-Your-Customer tools. One of the first remote identification systems appeared back in 2002, and this system allowed to pass identification on the Internet, to sign electronic documents, to participate in electronic voting, use the services of banks and government agencies.

Conclusions

Assessing existing international technologies and mechanisms in the sphere of combating the legalization of money obtained through money laundering and financing of terrorism, we can say that there are enough tools to concentrate the efforts of all parties of international relations on solving the above mentioned problems.

At the same time, it should be noted that the growing interdependence of the world economy, the increase in the speed of distribution of funds, coupled with the reduction in the ability of Member States to regulate or at least track these processes, makes governments and international organizations seek various ways to control financial flows, including illegal. Such

a need creates a dilemma. Either to follow the path of toughening national legislations, international standards, or to allow criminal and terrorist organizations to use all the "advantages" of globalization without any restrictions. Considering existing international initiatives in the field of combating money laundering, it is easy to assume that the Member States are most likely to decide to follow the first path.

Existing agreements, various organizations and institutions are designed, to a greater extent, to neutralize the technical processes of money laundering, but do not at all the underlying root causes of the problem. A number of factors impede its solution, many of which have political significance, and if the fight against the legalization of money laundering is contrary to the interests of the state then there is always the possibility that some countries will put these interests above international requirements. In this case, the effectiveness of the measures taken to counter money laundering is difficult to assess as high.

The emergence of new technologies does not occur on its own, but fits into a wider tendency for a change in society as a whole. It seems that the main task is how these changes could be used for public - to build a more secure, transparent and competitive economy with minimal money laundering risks.

References

Byrnes W.H., Munro R.J. Money Laundering, Asset Forfeiture and Recovery and Compliance -- *A Global Guide,*· 2023

Button M., Hock B., Shepher D. Economic Crime From Conception to Response, 2022

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2018.284.01.0022.01.ENG

Edelbacher M., Kratcoski P.S., Theil M., Financial Crimes: A Threat to Global Security, Advances in Police Theory and Practice, *CRC Press*, 2012 – 146.p

Feral-Shuhl, C., Paul, C. (2015). Peut-on protéger la vie privée à l'heure du numérique?. *En ligne sur le site web du Cabinet d'avocats Feral-Shuhl/ Sainte Marie* : http://www.feralavocats.com/fr/publication/peut-on-proteger-la-vie-privee-a-lheure-du-numerique

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations https://www.fatfgafi.org/publications/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

Parkman T. Mastering Anti-money Laundering and Counter-terrorist Financing, 2020

Perlman L. The Use of EKYC for Customer Identity and Verification and AML. *Focus Note*, 2019

Pollari, I. The rise of fintech opportunities and challenges. *Jassa*, 2016, (3), 15-21

Puschmann, T. Fintech. Business & Information Systems Engineering, 2017, 59(1), 69-76

Riemer, K., Hafermalz, E., Roosen, A., Boussand, N., El Aoufi, H., Mo, D., & Kosheliev, A. The Fintech Advantage: Harnessing digital technology, keeping the customer in focus. University of Sydney, *Business School and Capgemini*.2017