



RISKS OF THE USE OF FINANCIAL TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING: TYPOLOGIES AND FORECAST

Otaboev Bobur Ibrat Ugli

**Lecturer, Department Of Criminal Law, Criminology And Anti-Corruption, Tashkent State
University Of Law, Uzbekistan**

ABSTRACT: - This article is devoted to the risk of using new technologies in the legalization of criminal proceeds and the financing of terrorism. Discusses issues of blockchain technology and other innovations that are used for criminal purposes. Various practical examples are considered using new financial technologies, and a forecast is made based on the analysis done.

KEYWORDS: Money laundering, financial technologies, blockchain, bitcoin, terrorist financing, AML/CFT, cryptocurrencies, FATF Recommendations, risk.

INTRODUCTION

In recent years, the world has developed and continues to develop rapidly. In this regard, the improvement of financial technologies is no exception, because they have a significant impact on the development of the financial industry and the growth of the country's economy as a whole. Financial innovations are not only attractive and convenient products

for consumers, but at the same time, they create new problems in combating money laundering and terrorist financing, and pose new challenges for specialists in improving the system for combating money laundering and terrorist financing (AML / CFT) and world practice in this area. Today, the acceleration of the execution and processing of transactions, the increase in the number of cross-border transfers, the availability of financial services,

**“RISKS OF THE USE OF FINANCIAL TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING:
TYPOLOGIES AND FORECAST”**

the emergence of high-tech financial technologies, including blockchain technology and cryptocurrency based on it, as well as the vulnerability of the financial system and AML / CFT legislation to new threats, increase the risks of using these technologies for ML/TF purposes.

Financial technologies are developing every day, and the risks associated with them are growing accordingly. Based on the speed of improvement and global distribution of modern financial products, and the low level of legal regulation of the management of these products, then we can say with confidence that they will inevitably affect the AML/CFT sphere. It is not for nothing that the Financial Action Task Force on Money Laundering (FATF) in its standards gives a separate recommendation (R.15), which states that financial institutions need to identify and assess the risks of money laundering or terrorist financing that may arise in connection with the development of new products and new business practices, including new transfer mechanisms, and the use of new or developing technologies for both new and existing products, and take appropriate measures to control and mitigate these risks. This recommendation proves that new technologies are indeed risky for the AML/CFT system and the FATF call is justified, the implementation of which can reduce the risks of ML/TF.

The risks of new financial technologies depend on several factors. First, the global spread and availability of financial technologies makes them riskier. Recently, financial innovations have been widely distributed not only among developed countries, but also in developing and less developed countries. New tools have ceased to be an element of luxury, and be available only to a certain circle of people, but

have become publicly available to everyone around the world.

Secondly, the demands of society began to take on a different character. Considering that with the development of technology and the revolution in terms of technology, life has accelerated significantly, accordingly, consumers have begun to demand the rapid provision of services. As a result, various financial products and services have appeared, such as online banking, international money transfer service, etc.

Thirdly, government agencies themselves are interested in using innovative technologies, since their use in the financial sector makes it possible to track assets and counteract the shadow economy. The fact is that the use of cash is still relevant, and the spread of new financial technologies that are convenient for managing money will allow consumers to switch to cashless payments, thereby reducing the use of cash, the control of circulation of which is a very difficult process.

Fourth, the cross-border nature of financial products. Nowadays, cash is increasingly being squeezed out of the economy due to new ways of working with non-cash means of payment (online banking, plastic cards, online wallets, etc.). Today, an individual with a card can pay for any services from anywhere in the world and transfer money to anywhere in the world. This makes it difficult for regulators to keep track of funds, as there is a question of legal regulation in different jurisdictions. For example, if the money is transferred to countries with a high risk of money laundering and terrorist financing (North Korea, Iran), then tracking them will become extremely difficult.

Fifthly, the centralized monetary system, which allows government agencies to control

**“RISKS OF THE USE OF FINANCIAL TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING:
TYPOLOGIES AND FORECAST”**

the funds in the accounts and freeze or confiscate at any time, large commission payments to banks have led to the emergence of decentralized cryptocurrencies based on blockchain technology, which are rapidly developing.

At present, there are many different ML/TF typologies with the use of financial technologies. One of them is a money-laundering scheme with the help of the gambling sector. The use of cashless payments and the opening of electronic accounts have expanded the possibilities of the gambling sector, allowing you to open online gaming platforms on the Internet. Online gambling is inherently a cross-border activity. Various gambling platforms are registered in different jurisdictions. For example, a gambling site (online platform) may be registered in one country, while the server may be located in another. Financial transactions and management of the Internet gambling site may be carried out from a third jurisdiction. As a result, regulation of this sector involves multiple stakeholders and legal systems, sometimes leading to legislative and jurisdictional gaps that can be exploited for ML/TF purposes.

In the MONEYVAL Typology Report 9 dated April 11, 2013, several possible typologies using the gambling sector are presented. For example, a money launderer colludes with the operator of an offshore gambling site, deposits the proceeds of crime into a gambling account, and withdraws the funds as winnings. The site operator keeps a percentage of the proceeds as a commission, and the criminal declares the winnings to the tax authorities and then uses the funds for legitimate purposes. Another of the common gambling schemes, where the money launderer colludes with professional gamblers to place illegally obtained funds on

gambling sites, and the players keep a commission on winnings before transferring the remaining funds to the criminal, is also actively used by criminals.

The above typologies are among the most common online gaming sectors that are actively used by criminals for ML/TF purposes. These typologies are not exhaustive. There are many different typologies not only using online gambling platforms, but also using other financial technology innovations.

When it comes to financial technologies, one cannot help but dwell on cryptocurrencies based on blockchain technology. In recent years, cryptocurrencies have developed rapidly and have reached the point where in some countries, merchants in some stores accept cryptocurrencies (mainly Bitcoin) as a means of payment. The current situation in the world, the global prevalence of cryptocurrencies, transparency, availability without restrictions, the instantaneousness of transactions, the implementation of which is possible all over the world, the anonymity of the parties when making transactions, make this financial product attractive to criminals for the purpose of committing ML/TF.

The above characteristics of cryptocurrencies create favourable conditions for both the legalization of presumptive income and the financing of terrorism. Launderers invest money received from criminal activities into crypto-currencies and convert them into fiat money in offshore-registered crypto-exchanges. Crypto exchanges are already spread all over the world, and in some countries, there are strict requirements for them, ranging from licensing this activity to identifying crypto exchange participants and their counterparties. Therefore, launderers in many cases convert their cryptocurrencies in crypto exchanges registered in offshore zones.

**“RISKS OF THE USE OF FINANCIAL TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING:
TYPOLOGIES AND FORECAST”**

Money laundering is not the only crime that can be committed with cryptocurrencies. The employees of the FIU and law enforcement agencies of the countries have registered cases of financing terrorism using cryptocurrencies. The question arises, how can terrorists be financed with the help of cryptocurrencies? Many countries (including the Russian Federation) have regulated cryptocurrencies as property and as an object of civil circulation. If you pay attention to the requirements of the FATF and other international conventions on incriminating the financing of terrorism in the national laws of countries, you can see that according to these documents, the transfer of not only funds, but also any other funds aimed at ensuring the existence, functioning of terrorist organizations and lone terrorists, direct or indirect provision or collection of any funds, resources, or other services to terrorist organizations or persons assisting or participating in terrorist activities. Based on this, we can say that the transfer of cryptocurrencies, being an object of civil circulation, is the financing of terrorism.

Although cryptocurrencies were created relatively recently (2008), but today, many ML/TF crimes using cryptocurrencies have been solved by FIU employees and law enforcement agencies around the world. One of the most resonant cases in the history of mankind with the use of cryptocurrencies is the "Aleksandar Vinnik Case", where he is accused of money laundering, fraud and other fraud with cryptocurrencies. According to the data, in 2011 he founded the BTC-e online crypto exchange, which converted cryptocurrencies into fiat money. According to American law enforcement agencies, Vinnik was involved in a hack in 2011-2014 of a similar Mt. Gox, registered in Japan, as a result of which several hundred thousand bitcoins

were stolen (at the exchange rate for the summer of 2017, this amount was equivalent to almost \$2 billion). He legalized these funds with the help of his BTC-e crypto exchange, by converting them into various currencies, including dollars, euros and rubles. Vinnik is also charged with providing money laundering assistance through his crypto exchange to criminal groups, including drug dealers. According to American experts, the turnover of the exchange ranged from 4 billion to 9 billion US dollars.

In addition, at the present time, cryptocurrency has begun to be used not only in money laundering, but also in other predicate crimes. One of them is the case of two investigators of the central apparatus of the FSB of the Russian Federation, Sergei Belousov and Alexei Kolbov, accused of extorting a particularly large bribe from a person under investigation. An interesting fact is that the bribe was given by Bitcoin. This fact suggests that in the future the probability of laundering this money was closer to 100%, since they would still have converted it to fiat currency in a crypto exchange, thereby giving legal character to these funds.

As we can see, financial technologies have developed well enough to commit major criminal acts using them. Today, the FIU and law enforcement agencies are uncovering and preventing many ML/TF crimes using financial technologies that have caused or could have caused millions of dollars of damage to the global economy. And these are just cases that have been solved or prevented. Given that an indefinite number of crimes using new financial technologies remain latent, one can imagine how high the level of harm that is or may be caused in the future. Unfortunately, the development of financial technologies and their legal regulation are not at the same level.

**“RISKS OF THE USE OF FINANCIAL TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING:
TYPOLOGIES AND FORECAST”**

The fact is that countries, for various reasons, do not find the possibility of legal regulation (as happens with cryptocurrencies due to the cross-border nature of the product and jurisdictional problems) or simply do not have time due to the rapid development of this industry and the inventions of more and more new financial innovations. . Therefore, predicting the future, we can say that financial technologies will develop even more strongly, and taking this into account, the full regulation of the activities of financial technologies today, given the current opportunities and in the coming years, is a very difficult task, although tremendous work is being done in this direction.

Based on the foregoing, we can say that the level of risk of using financial technologies is quite high due to the various factors listed above and there are a number of different ML / CFT schemes with their use, which increase every day and criminals find more and more new ways of ML / FT, including using cryptocurrency. The current situation with fintech suggests that it needs to be fully regulated, although it is a difficult task at the moment.

REFERENCES

1. Criminal Code of the Republic of Uzbekistan. Tashkent, Adolat, 2021.
2. Холиков Ф. У. ЎЗБЕКИСТОН РЕСПУБЛИКАСИДА ИШТИРОКЧИЛИҚДА СОДИР ЭТИЛАДИГАН ЖИНОЯТЛАРНИ КВАЛИФИКАЦИЯ ҚИЛИШ МАСАЛАЛАРИ //Eurasian Journal of Law, Finance and Applied Sciences. – 2022. – Т. 2. – №. 4. – С. 16-20.
3. Qunduz Rozimova. Some Features of Improving the Penal Institution for Several Crimes in the Criminal Law of Uzbekistan in the Fight against Corruption. Journal Of Adv Research in Dynamical & Control. Vol.

**“RISKS OF THE USE OF FINANCIAL TECHNOLOGIES FOR MONEY LAUNDERING AND TERRORISM FINANCING:
TYPOLOGIES AND FORECAST”**