Threats to financial security

Boyko Petev [*] [1] [A]

*Corresponding author: [1] Associate Professor, Doctor, a Lecturer at Higher School of Security and Economics, e-mail: boykopetev@gmail.com, ORCID: 0000-0002-9786-1979

[A] Higher School of Security and Economics, Plovdiv, Bulgari

Received: September 1, 2022 | Revised: September 25, 2022 | Accepted: September 30, 2022

DOI: 10.5281/zenodo.7129002

Abstract

The study of threats related to financial security and the possibilities to minimize and eliminate the negative impacts and encroachments of fraud attempts on people, companies, the state and the EU are current security issues and challenges. The Internet has become a hyper-attractive place for criminals, as they often use tricks and promises to obtain money or valuable banking information. The techniques and tactics used are increasingly innovative and difficult to detect and deserve a thorough review in order to protect potential victims of bank fraud from threats.

Key words: threats, fraud, financial security, money laundering, terrorist financing, offshore accounts, bitcoin.

Introduction

This article makes an attempt to study **the threats related to financial security** and the possibilities to minimize and eliminate the negative impacts and encroachments of **fraud** attempts on people, companies, the state and the EU, are current security issues and challenges in every country and throughout the EU.

Results and Discussion

Anti-Fraud Policy

In order to protect the interests of individuals, businesses, the state and the EU regarding fraud in EU countries, a special EC anti-fraud policy has been adopted. The main objectives of this policy are related to raising awareness and strengthening fraud prevention measures through risk assessment and developing fraud detection capacity, providing guidance to EU countries to strengthen cooperation with the European Anti-Fraud Office (OLAF). OLAF is the EU anti-fraud body, authorized to investigate all suspected cases of fraud, corruption or serious irregularities in the EU institutions, or among the beneficiaries of EU funds. Reports to OLAF can be submitted anonymously in any of the official EU languages. The Office prepares annual reports on anti-fraud activities affecting EU funds in the previous year.

EU anti-fraud program

The EU's anti-fraud program funds activities related to technical and operational assistance for investigations, specialized training and scientific research to prevent and combat fraud, corruption and other illegal activities affecting the EU's financial interests. With the help of the accumulated knowledge and experience, OLAF helps the authorities responsible for the management of EU funds on the types of fraud, trends, threats and risks to protect the financial interests of the European Union by preventing fraud of all kinds and for the financial security of the countries. The protection of the EU's financial interests is carried out through effective prevention and countermeasures against attempts at fraud and abuse, building a common approach to improve interaction with European partners, as well as against ineffective management or use of EU funds.

Fraud in EU countries

The establishment and maintenance of effective supervision and continuity of the operation of the payment systems and the infrastructure of the financial institutions – banking and non-banking – is a guarantee for the effective implementation of a set of measures to prevent money laundering and counterfeiting, as well as the financing of extremist, terrorist and other activity prohibited by law.

Fraud in the EU financial system is a **crime** under national criminal law and should be prosecuted to the full extent of the law.

"**Money laundering**" is related to the fight against the penetration of criminal capital into the legal economy and the financing of terrorist activities as one of the main challenges to national and international financial security in the 21st century. "Money laundering" is the process by which "dirty money" generated through criminal activity appears as "clean", as if it had been obtained from legal activity. The term "money laundering" is relatively new, but this activity is not new. Whenever there is a need to hide a financial transfer, something like money laundering occurs. To launder the money generated by their criminal activities, the launderers have a wide choice and options. The scheme, where a combination between a bank and a business is used, can be considered as the main one for money laundering, and everything else is its variants.

It is difficult to determine the channels for **terrorist funding**. The prevailing opinion is that of the authors who point to the gray economy and its varieties as a way of financing terrorism (drug trafficking, money laundering, etc.).

A major channel of terrorist financing is through "unregulated activity", which can be distinguished into:

- ✓ Underground economy, which includes production of products or provision of services, which is not prohibited by law, but is deliberately hidden from the public authorities – tax, customs, social, statistical, etc. The proceeds from these sales are used to exchange /barter/ purchase weapons, ammunition and others. Shadow economy; It is an activity, as a result of which, for financial reasons, the receipt of certain revenues does not become known to the state authorities, and these funds are directed to the achievement of certain goals by terrorist organizations;
- ✓ Illegal economy, including various types of entrepreneurship that are prohibited by law. The illegal economy produces such products or provides such services, the production, sale or distribution of which is generally prohibited by law. An example is the drug trade;
- ✓ Informal sector, including a set of activities carried out due to the need to seek one's own livelihood due to the fact that other sectors of the economy (agriculture, large modern enterprises, public-administrative activities) are not able to hire workers at the rates at which it grows and is offered;
- ✓ The informal economy includes production that is not covered by statistics or tax and customs authorities, and also provides funds for terrorist organizations. Black economy; The black economy covers unreported production by registered enterprises for the purpose of avoiding taxes, as well as the production of unregistered production units;
- ✓ The hidden economy includes the undeclared legal production of goods and services, the production of illegal goods and services, and the incomes from theft at the workplace. When receiving funds from some of the abovementioned activities, these funds must be legalized. This is done through the so-called money laundering. Very often, money laundering and terrorist funding are mentioned in the same context, and the control actions, the established regulatory institutions and the normative documents adopted at the international level are intended to serve both the fight against money laundering and the prevention of the financing of terrorism. It is important, however, to point out that these two phenomena represent two separate and different criminal acts.

Intersections of the financial system and financial security

The question of the intersections of the financial system and financial security, economic security, environmental security (Tuntova, 2022, pp. 906-916), has a key role and importance, as it is related to countering phenomena such as money laundering and terrorist financing. For their part,

they are phenomena that are major challenges to national and international economic and financial security in the modern world to limit and prevent the penetration of criminal capital into the legal economy and the financing of terrorist activities.

Threats to the economic and financial security

Threats to economic and financial security include:

- **Investment fraud** is related to the profitability of the investment opportunities, promises of a quick return on the investment, and that it is safe. They are found in the trading of shares, bonds and the sale of alternative energy, investing in land (most often abroad). Prevention of such investment fraud requires the use of the services of specialists in the given field or unbiased financial advice;
- **Corporate fraud**, or "White-collar" fraud, is a type of fraud that is committed by managers or employees (most often financiers) by dishonestly and illegally abusing the trust of a company by transferring assets through financial transactions to given companies in the country and abroad; accounting fraud; forged (falsification) of financial results; embezzlement and racketeering; illegal access to a computer network and others;
- **Frauds, through forged bank safes**, collecting personal and financial data of individuals, through a variety of methods, by using phishing emails containing a link to forged bank websites that almost look like an authentic web page;
- **Fraud with electronic payment document**, using illegally obtained credit and debit cards to siphon off funds. Since ATM withdrawals are limited, the stolen cards are used to make purchases in large retail chains, using post-terminals where there is no ceiling on the payments;
- **Fraud by carrying out banking operations without the knowledge of the partners**, in which the fraud is committed by one of the partners who uses company funds for personal needs. If the amounts are larger, the partner usually provides as collateral the company's property;
- **Using the Internet for bank fraud** is most common in cases where customers are attracted through social networks to conduct attractive surveys and for quick profits, promising significant cash prizes or discounts on purchases, just by filling out a survey card. There are almost always winners. To claim the prize, the winner must transfer a fee and provide personal and banking information, which fraudsters then take advantage of;
- **Fraud through online shopping** is a type of shopping that is gaining momentum and is preferred by many people who research the offers or the desired product. Before the payment is made, it should not be by post, but using credit and debit cards and websites;
- **Fraud through fake banking websites** (phishing email) is another type of fraud that is done by creating a duplicate of an existing webpage of a major bank or credit company;
- **Business Email Compromise (BEC) scams** are a type of cyber fraud. The Association of Banks in Bulgaria warned of seven such types. Compromised business email scams appear to be sent by a company executive. Fraudsters impersonate the person and trick the person into paying a fake invoice or making an unauthorized transfer from the company's business account. In business correspondence scams, hackers compromise the official email correspondence and change the information in order to harm businesses, companies, NGOs, etc. The scheme works in the following way: the sent emails usually contain invoice with an account to which the money should be transferred. The customer pays it to the replaced account, and the victim is left without the paid funds;
- **Scams through bank phishing emails, phishing text messages and voice phishing** is a type of fraud where attempts are made to trick individuals into sharing their personal or financial information which can then be used for criminal purposes. They are carried out through:
  - bank phishing emails that are very misleading. At first glance, they appear identical to actual correspondence between banks and customers;
  - phishing SMS - fraudulent text messages are used;

– voice phishing – as in the above cases, fraudulent messages are exchanged over the phone.

➢ **Social engineering fraud** is based on cybercrimes and means trickery and manipulation of the victims and attack on their psychological balance. Most often the crime is committed using phishing scams, phone calls or email crimes. The scammer calls or emails a help desk and pretends to have forgotten his password, making up a plausible story about it. The story convinces the customer service representative to change the registered email address. For this purpose, the scammer will report it and then reset the password. In this way, the scammer will get hold of his target's profile;

➢ **Bank fraud with invoices** is when fraudsters pose as suppliers and ask the recipient to pay their invoice to the wrong bank account controlled by them. They declare that they have changed their bank details and want the recipient's bank account on future invoices to be changed. In this way, his account is controlled by the fraudsters;

➢ **Identity theft** is the fraud that most often occurs with the theft of personal data, which can be acquired in many ways (Facebook, and other social networks), when concluding contracts for mobile and other services, etc. They are used to falsify the necessary documents that enable withdrawal of money over the counter after the loan has already been approved over the Internet.

The Bulgarian legislation has provided penalties for crimes against the financial, tax and insurance systems, through the Criminal Code (Criminal Code, 2022, Art. 253, Para. 1, 2 and 3). The code stipulates imprisonment from 1 to 8 years and a fine from 5,000 to 25,000 BGN.

Benefits and problems of offshore accounts as a threat to financial security

The benefits and problems as threats can be systematized as follows:

➢ One of the basic principles of financial freedom is to keep your money outside the jurisdiction where you earn it. Especially in countries like Bulgaria, where governments and laws change every four years, and sometimes much more often. The popular solution to this problem today is the so-called offshore accounts, which in brief work as follows: You pay about $ 2,000-3,000 initially to an agent who registers a company through another local agent in the offshore jurisdiction. Then the company opens a bank account, and you have to find a way to transfer the money there. Not a trivial and cheap undertaking, considering the legal requirement all transfers to offshore accounts to be taxed at 10%. Even if you manage to overcome these obstacles, several serious problems remain: offshore maintenance costs about $1,000 per year, so it is only an option for more substantial sums;

➢ a lot of paperwork;

➢ problems with the use of your money deposited in the offshore account: it happens most often with a credit card, which, however, does not have to be in your name, if you do not want to make the whole exercise pointless;

➢ enhanced checks wherever you decide to use the company. Those who have dealt with the subject can certainly think of many other obstacles, but the main problem is that you are constantly gnawed by a sense of uncertainty about your money: whether one of the agents will disappear, whether the Americans will decide to close the jurisdiction, won't you suffer the fate of the Cypriot offshore companies that lost 20% of their deposits a few years ago.

All of these drawbacks pale in comparison to the most important catch in the entire system: have you ever considered the fact that your money held in any bank account is not really yours? It is property of the bank that has signed a contract with you to give you access to it in strictly defined ways (credit cards, online banking, visiting branches), only at certain times and only up to certain limits. And all this for a fee – for keeping your money in the bank; for spending them.

Offshore areas are a problem of the global collective decision-making, part of the present and the future. There is a lack of awareness, will, mechanisms and authority for the abolition of offshore financial centers in our time, and the "devil's advocate" can come up with 50 arguments against any proposal in this direction. It seems that this is another in the list of global problems that humanity cannot come together to solve, along with global warming, nuclear weaponry and others. Perhaps the new world financial order could consider addressing the cause rather than the symptoms – prudent

government spending, transparency in public finances, curbing corruption and increasing the efficiency of the public sector would perhaps reduce debt levels and high tax rates in the developed world so that the corporations and the wealthy are not forced to hide their earnings. I hope this is the way of a new "new global financial order".

Advantages of the Bitcoin as an offshore account

If you take the time to read more about Bitcoin, you will realize that it is completely free, accessible to everyone, independent bank for your money. If you open a wallet on one of these sites, there's no one between you and your bitcoins in the way the banks sit between you and your money. Your Bitcoins are secure as long as you can protect your private key. And here the possibilities are many – you can do that on paper, on a hardware device, in an insured wallet, in your brain, and why not by using a multisign wallet, in which case even if your key gets stolen, you are still safe. Of course, until recently, there was the problem that once we converted our money into Bitcoin, we didn't have much to do with it other than keep it in a safe place and hope that its price would go up. However, this is no longer the case…

Let's look at the most recent conquests of Bitcoin. Once converted to Bitcoin, your money is available to you in all countries of the world, through services such as https://crypto.bg, which offer local currency in exchange for Bitcoin. So you don't have to carry cash with you through customs, you don't have to worry about your credit card limits, you don't have to worry about your card being skimmed and your money stolen. In the latter case, although after some time and headaches VISA or Mastercard will reimburse you, you are left without funds in a foreign country and have to resort to your family or friends to send you money through WesternUnion at the cost of huge commissions.

You can now spend your bitcoins at growing number of business (even those using PayPal) that accept bitcoin as method of payment. Even if a merchant doesn't accept bitcoin, there are plenty of services that offer instant bitcoin top-up credit cards. You can immediately spend them through it. In addition, the card is issued in your name and is applicable worldwide without problems.

The main problem with bitcoins is their still volatile price. Today you can buy them at $ 220 per bitcoin, and tomorrow when you have to spend them, the price could be $ 1800. To this problem there are the following solutions, you need to understand that the price of Bitcoin cannot be zero. If you take this for granted, it follows that no matter how much the price falls, it will eventually reach its bottom – the biggest pessimists say it will be around $ 80, but more realistically the bottom will be around $ 150. If you plan in a longer term and invest your money in portions whenever there is $10-$20 drop in the price, soon the average purchase price of your bitcoins will be lower than the market price. Thus when you spend them, in addition to the listed benefits, you will also profit from the Bitcoin investment itself, if you still don't want to expose yourself to its volatility, you can transfer your Bulgarian currency to gold, dollars or other currencies and precious metals – completely anonymously – through sites like Bitreserve. If you don't want to trust Bitreserve (despite their innovative procedures for full transparency), you can use decentralized solutions like BitShares.org. In both cases, you keep your money in your chosen asset completely anonymously. Because the registration of this type of account requires only an email and a password. If you try a little harder, even the FBI hounds couldn't link those accounts to you. Again, with these types of services, you don not hold Bitcoin. You hold assets of your choice that are easily accessible through the Bitcoin network. A much better solution than buying physical currencies or metals, given the problems of their storage, cross-border transfer and liquidity.

The cryptocurrencies inspire both hope and chilling worry. Today, many are hopeful that the future of money is shaping up to be independent and free from the standard banking system. Until about ten years ago, when the world was gripped by a deep financial crisis, no one could have imagined such an outcome. There are over a thousand types of cryptocurrencies, the most famous being bitcoin, Litecoin, Ethereum, and among the unpopular are newcomers like Zcash and Yubikey. The veteran here is undoubtedly Bitcoin, which took the world by storm with its powerful vision in 2009. If we were to compare the traditional offshore accounts with the rapidly emerging crypto wallets as an alternative to tax avoidance, as a natural continuation of the evolution of the financial

system, or rather as a reflection of the problems that our society and governments of the individual countries are failing to deal with, surely the world of cryptocurrencies is limitless.

Today, in the 21st century, when the world is getting smaller, the Internet comes as a successful alternative where you can hide not only your money and identity with one click, but do all this without unnecessary documentation and approvals from institutions. Let's not forget that ultimately we choose how to use the benefits and power that blockchain and cryptocurrencies give us. We are the ones who choose what to do with the knowledge we are given, and that in itself is neither bad nor good. Our future actions will determine whether we have used it to build a fairer financial society or whether we will continue with the same greed to destroy not only our countries but also the environment.

The conclusion that needs to be drawn is that Bitcoin is an innovative currency that is not regulated by governments, like any other cryptocurrency. Through cryptocurrencies, payments can be made very quickly and at almost no cost. Among the advantages of Bitcoin is the fact that the virtual currency avoids the main problem characteristic of conventional currencies, namely inflation. One of the big advantages is anonymity. No one knows how many Bitcoins a person owns, or what transactions he uses it for.

Bitcoin helps the miners make profits, which in turn keeps the system running. In the beginning, it was easy to mine large amounts of Bitcoins, but as the popularity increased, the possibility of large profits began to decrease, even in some cases, some miners lost money. People are always innovative and manage to handle any situation and find a way to cheat the system. Miners join forces in pools and thus have a higher chance of profit. Bitcoin owners should be very careful and should take the necessary measures to preserve their ownership by using well-secured crypto wallets.

Bulgaria is second in the world in possession of Bitcoins, which could be used to pay the external debt. At the same time, with the development of the cryptocurrencies, the price of Bitcoin rises and falls quite quickly and can play a bad joke on us. The caution of the central banks comes from the fact that the cryptocurrencies are unregulated and this provides greater opportunity for anonymity and fraud. At the same time, banks are losing billions in taxes and transaction fees as consumers prefer cryptocurrencies as a means of payment on the Internet.

Scientific interest is the comparison of the classical concept of financial sovereignty – as the absolute, indivisible and permanent power of the state over its territory – and the modern content of this principle. This content is conditioned by the globalization, by the universal nature of human rights and by regional integration. In the balance between these principles and phenomena, the modern concept of financial sovereignty and the changed role of the state in the established world financial order is outlined. On this basis, specific measures should be taken on the role of the state regarding fraud, the differentiation of various problems related to the national security (Kolev, 2022, pp. 33-36), which cause irreparable financial damage, both in global and in European, national and regional aspects.

Conclusions

The Internet has become a hyper attractive place for criminals. They often use tricks and promises to obtain money or valuable banking information. The techniques and tactics they use are becoming increasingly innovative and difficult to detect, and deserve a thorough review in order to protect the potential victims of bank fraud.

References

Criminal Code, (2022). SG No. no. 26/02/04/1968, last amended SG. No. 53 of July 8.

Kolev, V. (2022). *Specification of intra-city transportation in view of the national security in the Republic of Bulgaria*. National Security Magazine, Sofia, Victory Izdat EOOD, issue 11, pp. 33-36, Available from : https://nacionalna-sigurnost.bg/broi-11/

Petrova, N. (2022). The effective tax control of cryptocurrency transactions as a guarantor of the financial security of the state, National Security magazine, Sofia, Viktori Izdat EOOD, issue 12, pp. 13-17, Available from : https://nacionalna-sigurnost.bg/broi-12/

Tuntova, A. (2022). Ecological security – challenges and opportunities, Collection of reports from the annual university scientific conference, June 30 - July 01, Electronic edition, IC of NSU "Vasil Levski", Veliko Tarnovo, pp. 906-916, ISSN 2367-7481.