ANTI-FRAUD TECHNOLOGIES IN E-BANKING

Daria Kibets, National Aviation University
Olena Lepei, National Academy of Internal Affairs
Oleksii Prokopenko, Kharkiv National University of Internal Affairs
Alina Chorna, Kharkiv National University of Internal Affairs
Mykola Shelukhin, Mariupol State University

ABSTRACT

The article outniles the advantages of electronic banking and possible negative phenomena (risks) that may arise in the process of using banking services. Particular attention was paid to the causes of fraud in the functioning of electronic banking, as well as the objects of encroachments of fraudsters in this area. The legal basis for resolving the issues of combating fraud in the field of electronic banking with regard to international standards, namely the experience of the European Union, was studied. The objectives of an effective fight against fraud in the banking sector were disclosed, taking into account the provisions of the Directive of the European Parliament and of the Council On combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, 2017. Attention was paid to the settlement of issues of combating fraud in the field of banking services in Ukraine, in particular, attention was focused on the activities of the EMA Association, as the national representative of Ukraine in EAST - European Association for Secure Transactions. The problematic aspects of the return of funds lost by a client of the bank from fraud on the part of third parties were identified.

Keywords: Fraud in the Banking Sector, E-Banking, Anti-Fraud in E-Banking.

INTRODUCTION

In modern conditions, among the many factors that influence the success of the economic development of any country, an important place is given to a developed banking system. The effectiveness of the functioning of the latter depends not only on the economy of the country, but also on global changes in the global space, which require its approach to the requirements of modernity. At the same time, for Ukraine issues of functioning of an effective banking system are caused not only by the European integration course, but also by the situation in the east of the country, due to which, as noted by Derevyanko et al. (2018), it becomes necessary to take into account the interests of the state and society while simultaneously searching for the credit resources of banks.

A special instrument, by which bank accounts are managed, is the electronic banking system. The introduction of such a system allows clients to carry out most banking operations independently if they have an Internet connection and the possibility of using a stationary computer, laptop or smartphone. However, despite the convenience of performing banking operations via the Internet, remote servicing of a bank's client may carry certain risks associated

with the possibility of fraud. The latter, in turn, not only cause damage to bank clients, but also have a destructive effect, manifested as a deterioration in the position of the bank in the banking market, and economic backwardness (Badejo et al., 2017).

Problem Statement

The introduction of innovative banking services via the Internet has led to the emergence of new types of fraud - Internet frauds, in particular, those which use involves the use of bank payment cards. Considering the above, an important issue is the security of banking operations in the electronic banking system, given the many existing types of fraud in this area. Thus, it seems relevant to study the characteristics of the commitment of fraud in the electronic banking system and combat this phenomenon.

LITERATURE REVIEW

The development of the global Internet and the rapid increase in the number of users has led to an increase in the volume of e-commerce, which also includes electronic banking. Today, a sufficiently large circle of consumers are convinced of the possibility of conducting banking operations without visiting the bank in person, and therefore prefer banking services on the Internet among other types of activities existing in it. At the same time, as noted by Abreu et al. (2015), e-banking services clearly have advantages in financial operations, but the threats and security "weaknesses" of using such services should constantly decrease. That is why the integration of fraud with all aspects of e-banking services requires the revision of traditional commercial paradigms that have prevailed in recent years.

Interesting is the position of Bhasin (2016), which argues that banks should involve their clients in active participation in their efforts to prevent fraud, because clients may be ready to go to competing banks if they feel they have remained unaware of these efforts. Since the banking industry is a highly regulated industry, there are also a number of external compliance requirements that banks must follow in combating fraudulent and criminal activities.

Reurink (2018) in its study draw attention to a number of recent events that caused financial frauds, among which fraud in the functioning of electronic banking is not an exception, namely: (1) development of new fundamental conflicts of interest and distorted financial incentive structures; (2) influx of inexperienced, trustful financial market participants; (3) increasing complexity associated with operations in financial markets, as a result of rapid technological, legal and financial innovations and the range of financial products, which are constantly expanding; (4) increase in the use of justified secrecy in the form of mystification of the trading models adopted by fund managers.

E-banking fraud is a threat to the security of the bank, which has both external and internal origin. If we consider the traditional banking services, then the object of infringement of fraudsters in this area is primarily money (or financial resources). In turn, if we take into account the sphere of electronic banking, the objects of fraud can be presented in the form of: (1) confidential information about bank clients, including payment card numbers, PIN codes, CVV code; (2) usernames and passwords of access to the electronic banking system, in particular, this applies to Internet banking and mobile banking; (3) financial resources of both the bank and its clients (Koivunen & Tuorila, 2015).

METHODOLOGY

The methodological basis for the study of the issue of combating fraud in the field of electronic banking consists of the following methods. The method of structural and functional analysis was used to determine the causes of fraud in the field of electronic banking and its main types. The comparative and legal method was used in the study of European standards to combat fraud in the banking sector, established at the level of EU legislation, and the norms of the current legislation of Ukraine in the fight against this phenomenon, including the functioning of electronic banking. The formal and legal method allowed the interpretation of legal norms to clarify their essence, in particular, the settlement of the return of funds lost by a bank client from fraud by third parties.

FINDINGS AND DISCUSSIONS

Studying the legal framework for resolving issues of combating fraud in the field of electronic banking, it is advisable to refer to international standards, namely the experience of the European Union. Thus, an important document regulating anti-fraud legal relations, which takes place in the banking sector, is the Directive of the European Parliament and of the Council On combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, 2017[1] (hereinafter-Directive). It is important to pay attention to paragraph 2.3 of clause 2 of the Directive, according to which non-cash payment fraud has very important cross-border detection both within the EU and beyond. A typical case might include skimming (copying) of card data in an EU country, creating a fake card using this data, and cashing with a fake card outside the EU to bypass high security standards. Increasingly, these crimes are committed online (Directive On combating fraud and counterfeiting of non-cash means of payment). The Directive rightly justifies why the goal of effectively combating such crimes cannot be sufficiently achieved by states acting alone or uncoordinatedly: (1) such crimes create situations where the victim, the criminal and the evidence may be in different national legal frameworks both within and outside the EU. As a result, it may take a lot of time for individual countries to effectively counter this criminal activity without general minimum rules; (2) the need for EU action has already been recognized through the creation of EU legislation to combat fraud and counterfeiting of cashless means of payment (Framework Agreement) (3) the need for EU intervention is also reflected in ongoing initiatives to coordinate EU member states 'activities in this area, such as the Europol task force that works on payment fraud, and the EU political cycle EMPACT on operational cooperation against non-cash payment frauds (Directive On combating fraud and counterfeiting of non-cash means of payment).

It should be noted that the Europol website contains information on the EU political cycle-EMPACT. According to the data posted in 2010, the EU introduced a four-year policy cycle to create greater continuity to combat serious international and organized crime, which requires cooperation between law enforcement agencies, other agencies, EU institutions and third parties. In March 2017, the Council decided to continue the EU's policy on organized and serious international crime for the years 2018-2021 aimed at resolving issues related to organized and serious international crime. Among the objectives of this policy are the prosecution of criminals involved in fraud and counterfeit non-cash means of payment (EU policy cycle-EMPACT)[2].

Regarding the regulation of the issue of combating fraud in Ukraine, it is important to note that the National Bank of Ukraine in 2018 developed Recommendations for reducing the risk of fraudulent operations. This is explained by the fact that today there is a high level of the number of cases of fraudulent operations using payment cards and unauthorized transfer of funds from client accounts that are serviced using remote service systems (Recommendations for reducing the risk of fraudulent operations[3]). This is confirmed by the statistical reporting submitted by banks to the National Bank of Ukraine (for example, in 2016-94.6 thousand fraudulent cases with payment cards in the amount of 177.2 million UAH, and in 2017-77.6 thousand cases in the amount of 163.7 million UAH), and an increase in the number of appeals/complaints of Ukrainian citizens regarding unreasonable write-off from accounts, non-return (or deliberate non-return) of funds to accounts of holder's payment cards (in 2016-1007 appeals of citizens, and in 2017-1287) (Recommendations for reducing the risk of fraudulent operations).

It is important to note that in Ukraine, in 1999, the Association EMA was created by banks, members of Europay International, to counteract fraud in the banking sector. Since 2012, the Association EMA is the national representative of Ukraine in EAST-European Association for Secure Transactions. The aim of EAST is to organize the international exchange of reliable information on current trends and statistical information on frauds in ATMs, terminals, and payment fraud. The purpose of the activities of national representatives from 35 countries of the world is to collect and provide such information regarding the country they represent (Association EMA in Ukraine, official website[4]).

The opportunity to withdraw fraudulent bank payments or to compensate losses as a result of such illegal actions to victims is presented as one of the main points of sale of the banking services system and, in particular, payment cards. However, whether a victim of fraud gets his/her money back or not, will depend on banking operations and ultimately on the contract between the bank and its clients, which depends on the specifics of national or international legislation (Becker et al., 2016). In Ukraine, the return of funds lost by a client of a bank from fraud by third parties is a very problematic issue, because in most cases the client, although unintentionally, but independently, discloses information about the banking details to fraudsters.

This is confirmed by the norms of the Law of Ukraine On Payment Systems and the Transfer of Funds in Ukraine and the Resolution of the Board of the National Bank of Ukraine On conducting operations using electronic payment facilities. According to cl. 14.16 and cl.6 of Section VI, the risk of loss is imposed on the client, who, after revealing the fact of loss of the electronic payment instrument, is obliged to immediately notify the bank in the manner provided by the contract (Law of Ukraine On payment systems and transfer of funds in Ukraine[5]; Resolution of the Board of the National Bank of Ukraine On conducting operations using electronic payment facilities[6]). However, an important event in 2016 was the fact that the VISA system introduced the "*principle of zero liability*" for holders of its cards. This principle provides for the return of funds stolen by fraudsters by a bank to a VISA card holder, subject to confirmation that the cardholder did not contribute to fraud.

RECOMMENDATIONS

The various forms of electronic banking that have been introduced recently have had a positive effect on banking services, which has made it economically viable and has increased the

efficiency of implementation. At the same time, such changes should also have a negative consequence, which is explained by the vulnerability of banks and their clients to fraudulent actions by third parties.

Countering fraud in the banking sector in Ukraine, including payment card fraud; the theft of private, confidential information in order to seize funds from real clients; illegal withdrawal of funds from a bank account; disrupting the operation of automated banking service systems, etc., is possible only by approximating legal regulation in this area with international standards for combating this phenomenon.

CONCLUSION

Today, an integral part of banking services in the functioning of electronic banking is the risk of fraud with the funds of bank clients. Its manifestation is mainly the theft of confidential data of clients in order to further access to their financial resources. A significantly large number of fraudulent activities in the electronic banking system has negative consequences, expressed in reducing the confidence of citizens in banking institutions, the reliability of the protection of their personal data and banking operations conducted using electronic banking, and the like.

The experience of European banks shows the effectiveness of implementing various ways to protect financial operations of the clients, among which an important place is given to authenticating the user using USB tokens, one-time passwords, confirming transactions using codes that are sent as SMS messages and the like. It is important to remember that the basis for the security of operations in the electronic banking system is, first of all, non-disclosure by clients of personal data associated with their bank card, its number, CVV code, pin code of the card, mobile phone number of the client, to which the card is tied with a username and password from the personal account if the person is registered in the Internet banking system. Such information very often opens the way for third parties to implement fraudulent actions with the client's funds.

ENDNOTE

1. Directive of the European Parliament and of the Council On combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (2017). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM: 2017:0489:FIN
2. EU policy cycle-EMPACT. Europol. URL: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.
3. Recommendations for reducing the risk of fraudulent operations: a letter of the National Bank of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/v3636500-18. [in Ukrainian].
4. Association EMA in Ukraine. Official website.URL: https://ema.com.ua/about/board.
5. Law of Ukraine On payment systems and transfer of funds in Ukraine, as amended up to Act of February 07, 2019. URL: https://zakon.rada.gov.ua/laws/show/2346-14. [in Ukrainian].
6. Resolution of the Board of the National Bank of Ukraine On conducting operations using electronic payment facilities (2014, as amended up to Resolution of September 09, 2016). URL: https://zakon.rada.gov.ua/laws/show/v0705500-14. [in Ukrainian].

REFERENCES

Abreu, R., Segura, L., David, F., Formigoni, H., Legčević, J., & Mantovani, F. (2015). Ethics and fraud in E-banking services. *In 2015 10th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6).

Badejo, B.A., Okuneye, B.A., & Taiwo, M.R. (2017). Fraud detection in the banking system in Nigeria: Challenges and prospects. *Shirkah: Journal of Economics and Business, 2*(3), 1-12 .

Becker, I., Hutchings, A., Abu-Salma, R., Anderson, R., Bohm, N., Murdoch, S.J., Sasse, M.A. & Stringhini G. (2016). International comparison of bank fraud reimbursement: Customer Perceptions and contractual terms. *Conference: Workshop on the Economics of Information Security (WEIS), 15*, 1-31.

Bhasin, M.L. (2016). Frauds in the banking sector: Experience of a developing country. *Asian Journal of Social Sciences and Management Studies, 3*(1), 1-9.

Derevyanko, B., Nikolenko, L., Syrmamiik, I., Mykytenko, Y., & Gasparevich, I. (2018). Assessment of financial and economic security of the region (based on the relevant statistics of the Donetsk region). *Investment Management and Financial Innovations, 15*(4), 283-295.

Koivunen, T., & Tuorila, H. (2015). Consumer trust relations with payment cards and banks: An exploratory study. *International Journal of Consumer Studies Banner, 39*(2), 85-93.

Reurink, A. (2018). Financial fraud: A literature review. *Journal of Economic Surveys, 32*(5), 46-72.

This article was originally published in a Special Issue 2, entitled: **"Business Laws and Legal Rights: Research and Practice",** Edited by **Dr. Svetlana Drobyazko**