Info-Communicative and Protective Function of the State as Combating Fraud using Sberbank Bank Cards

Igor Yu. Nikodimov[1,*], Igor A. Burmistrov[1], Tatyana N. Sinyukova[1], Elena A. Mironova[1] and Sergey I. Zakhartsev[2]

[1]*Department of Criminal Law Disciplines, Russian State Social University, Moscow, Russian Federation*

[2]*Department of Advocacy and the Organization of Law Enforcement, Russian State Social University, Moscow, Russian Federation*

Abstract: Financial crimes are defined as unfair activities that have become widespread in banking structures. The activities of financial fraudsters often have negative consequences before public rules are created that prohibit them. Intensive transformation processes in financial markets, their automation and virtualisation, the spread of remote interaction between banks and their clients, the influence of unauthorised persons on the software and hardware systems of banks, an increase in the number of cases and trading volumes determine the relevance of clarifying the essence of this phenomenon and the peculiarities of its manifestation in banking structures. The novelty of the study is determined by the fact that financial violations can be represented both in the structure of the current activities of banks and the process of interaction with clients and in the structure of expanding the list of services provided. The leading method to study this problem is the method of analysis, which allows to identify and comprehensively consider ways to counter financial crimes in banks to improve the level of financial security. The authors show that structurally, one should take into account, first of all, countermeasures on the part of customers, which often serve as a source of obtaining personal data. In this case, the state function is considered only as a security function for the purpose of possible punishment for fraudulent actions. The practical significance of the study is determined by the possibilities of structural implementation of combating financial fraudulent actions in the context of the development of the information society.

Keywords: Financial violations, fraud, banking structure, banking activities, financial security.

INTRODUCTION

There are such unacceptable for society methods of seising financial resources, such as: violent, fraudulent and theft. The largest losses in the field of financial relations are caused by financial crimes in banks, the basis of which is deception. A group of researchers led by P.-L. Chatain (Chatain *et al*. 2009) share the negative consequences, or problems, that financial institutions involved in illegal transactions may face, into reputation, operational and legal. When it comes to financial crimes, financial problems should also be added to the list. Financial crimes in banks indicate the inability of the latter to ensure their own financial security at the proper level. As a result, financial crimes become possible, which inevitably lead to the loss of financial resources and, ultimately, to the revocation of a banking license and bankruptcy. Moreover, the real price that banks involved in financial crimes may pay cannot always be expressed in terms of money alone. Loss of reputation and trust, lawsuits, stifling motivation of bank staff, breaking off business relationships, loss of banking market share and prospects are just some of the non-monetary consequences of financial crime in banks.

Solving the problems of identifying, counteracting and preventing financial crimes that each bank face is impossible without understanding the essence of financial fraud and formulating its correct definition. It should be noted that in the scientific community there is a fragmentation of views on the concept of “financial fraud”, as well as a lack of unity in approaches to determining its manifestation in banks. The scientific assessment of financial crimes is also ambiguous. It is believed that the fraudulent techniques are not original, that in order to “cheat” a bank, one does not need a lot of intelligence. It is noted that it rarely happens when a bank fraudster used something new and original in embezzlement. In contrast to this position, they note that fraud is a global phenomenon, which invents more and more new ways to “legally” receive money from banks. This emphasises the relevance, the necessity for constant work with scientific deepening of knowledge to identify financial crimes.

The dominant position regarding the awareness of financial crimes in banks primitives it, reduces it to a simple, ordinary financial crime (pulling banknotes from packs, substituting a counterfeit currency for real currency, losing a banknote during transfer, not depositing funds under a deposit agreement). Such awareness (through deception, abuse of trust and official position, using computer technology or false information) is the reason for inappropriate detection of

*Address correspondence to this author at the Russian State Social University, Moscow, Russian Federation; Tel: +7 495 255-67-67;
E-mail: nikodimov5253@kpi.com.de

E-ISSN: 1929-4409/20

financial crime. An expert assessment of the volume of implementation and detection of financial crimes, the amount of financial resources that were returned to the legal owners after its detection, and the number and status of financial fraudsters indicate a significant conceptual distortion of this phenomenon. When identifying financial crimes, quite often, without realising it, they try to recognise only theft, and all other actions remain outside the field of vision of researchers. It should be noted that this awareness reduces the effectiveness of the fight against financial crime in banks.

The main modern views on the phenomenon under study can be divided into: scientific-theoretical and practical-functional. The scientific-theoretical approach is an understanding of the phenomenon, starting from the collection of facts, their study and disclosure of individual laws to a holistic, logically constructed scientific theory that explains known facts and allows predicting new ones. The practical-functional approach is based on the characteristics of financial crimes by organisations whose activities are aimed at identifying, countering and preventing it.

LITERATURE REVIEW

The group of researchers led by C-R. Han reveal the essence of financial crimes from the point of view of criminology and draw attention to the fact that, among other things, legal actions are also an element of financial crimes. (Han, Nelen and Joo 2015). As a result of their research, scientists are of the opinion that financial crime is a criminological phenomenon, which is a criminal activity, and is expressed in a system of criminal and legal actions committed by deception or abuse of trust in the process of formation, distribution and use of funds in order to obtain material benefits. The International Federation of Accountants (2020) considers financial crime as the commission of unlawful acts in the field of monetary circulation through deception, breach of trust or other manipulations with the aim of enriching (Higgins 2012). From this perspective, financial crimes are not limited to deception and abuse of trust, but are marked by the use of manipulation (Aladwan 2020). Manipulation is an important element that allows correctly grouping financial crime tools (Hoffmann and Birnbrich 2012) This position limits the material purpose of financial crimes, which is not entirely correct, given the research results and opinions of various researchers (Stewart 2016).

Examining the motivational factors of fraud in the field of professional activity, the types are distinguished, among which special attention should be paid to “a strong desire to overcome the system” and “a feeling of discrepancy between wages and the degree of responsibility” (Baker, Cohanier and Leo 2017). The desire to overcome the system should not be associated with material needs; in a certain sense, this type may indicate attempts at self-realisation of an individual (Li *et al*. 2020). The subjective disagreement between the recognition of the ratio of the volume of wages and the work performed, which is sufficient motivation for the implementation of financial crimes, indicates not so much material motivation as an expression of a protest position (Tremblay 1986). About 95% of people are subject to manipulative, while only 5% are manipulative (Nanduri *et al*. 2020a). Thus, it is 5% of individuals who are capable of manipulating with the appropriate opportunities and awareness of impunity or avoidance of responsibility (Nanduri *et al*. 2020b). At the same time, such entities, committing fraud, including financial fraud, are not in a state of material need or other material motivation (owners and top managers of banks and managers, and owners, bank customers (borrowers and consumers of the bank's financial services) (Coogan *et al*. 2015). Intangible motivation in organising the seizure of financial resources explains the insignificant volumes of detection of financial crimes, even in such a regulated sphere as banking. The identification of such types indicates that not only material need is a driving force, one should also take into account the moral protest self-realisation (Hartmann-Wendels *et al*. 2009). Scientists also pay attention to the fact that fraud is a phenomenon of a moral order, which, in the authors’ opinion, adds arguments to the conclusion (Clinton 1996).

Financial crime is defined as any type of successful financial crime and other fraudulent activity that leads to the formation of sums of money that subsequently pass through bank accounts (Rahman *et al*. 2018). It should be noted that the receipt of sums of money, which in the future must go through bank accounts, very inaccurately characterise the phenomenon under study (Hollow 2014). Therefore, in the authors’ opinion, the elements of financial crime (crime, deception), highlighted by the author, only partially solve the problem of constructing a definition (Diadiushkin, Sandkuhl and Maiatin 2019). M.E. Lokanan (2019) proposes to understand a fraud as a person's use of his position for the purpose of personal gain through

the wilful misuse or abuse of the resources and assets of the "employing organisation". The author focuses on the use of his own, probably official position, for the purpose of personal enrichment. This, in the authors' opinion, outlines an important aspect of the studied phenomenon, but one-sidedly characterises its manifestation in banking (Hass, Vergauwe and Zhang 2019). In general, within the framework of the scientific and theoretical approach, the concept of "financial fraud in a commercial bank" requires further clarification in order to update it in accordance with changes in banking practices and consideration of its specific manifestations.

MATERIALS AND METHODS

The leading method for the study was the method of analysis, which allows identifying and comprehensively considering ways to counter financial crimes in banks to improve the level of financial security. The research materials were the strategies and the most significant developments in this direction among audit and consulting companies: Deloitte (The Deloitte Global ..., 2020), PricewaterhouseCoopers (PwC's Global Economic ..., 2020), International Federation of Accountants (2020) (in the field of audit and accounting) and the Association of Certified Fraud Examiners (2020) (in the field of investigation). The scientific and theoretical approach, as a general modern scientific awareness of the phenomenon under study, is represented by the following views: financial crimes are considered from the standpoint of forensic science and it is proposed to understand them as a complex of interrelated technologies of mercenary encroachments on the financial resources of the state, business entities and citizens committed through deception and malpractice. This opinion is a theoretical construction of the studied phenomenon from the standpoint of criminology, which, of course, requires adaptation when used in research in the field of banking activities.

Within the practical-functional approach, the position of PricewaterhouseCoopers (PwC's Global Economic ..., 2020) stands out, according to which fraud is identified with an economic crime and is defined as deliberate deception with the aim of stealing money, property and legal rights. The approach that associates financial crime with theft, in the authors' opinion, greatly simplifies the phenomenon under study and distorts its essential manifestation. International Federation of Accountants (2020) characterises fraud as obtaining an unlawful or illegal advantage: fraud is the deliberate act of one or more of the management personnel, those with the highest authority, employees or third parties, associated with the use of delusion to obtain an unlawful or illegal advantage ... In the authors' opinion, such a position does not so much define fraud as it tries to associate some of its features with any unfair economic and financial activity. Separate allocation of unlawful and illegal advantages, from the point of view of financial crime, is not of such a significant nature.

Association of Certified Fraud Examiners (2020) in its activities is guided by the following definition of the term "fraud": the use of official position for personal gain through the use of property or resources of the organisation. From this perspective, the phenomenon under study is due to purely practical expediency. At the same time, in the authors' opinion, a customer, when formulating the task of detecting fraud or financial crime, will not always have in mind the actual fraud. A customer is limited only by his own desire and understanding of what he aims to reveal. Therefore, this approach also does not solve the problem of defining the phenomenon under study as a scientific concept.

Note that the essence of the unification of the proposed model of financial crimes in banks is that it combines elements of financial crimes for the same functional purposes: methods of influence, methods of concealment, tools of seizure, tools of concealment, tools and methods of legalisation, etc. This allows to use it both to the types and kinds of financial crimes that are already found in banking practice, and to those that arise depending on the development of banking services, banking operations and technologies used by banks and financial fraudsters.

RESULTS AND DISCUSSION

Banking products and services, bank operations are adapted by fraudsters to use them as a tool for carrying out financial crimes. For this purpose, fraudsters introduce, in particular, a change of owners and a borrower (they can act as persons who assist a fraudster) after obtaining a loan for a front, low-quality collateral can be used, mistakes are deliberately made when registering financial relations that will lead to financial losses. A wide range of people is involved in the implementation of financial crimes in banks. They can be both conscious participants in financial crimes (persons who contribute to a fraudster) and persons who are used by a fraudster without realising their role.

When carrying out financial crimes, fraudsters try not to directly associate themselves with funds that are the subject of unfair appropriation. The funds are first directed to intermediate (assisting) persons. Only later, after legalisation and the creation of the corresponding legend, the funds obtained in an unscrupulous way go directly to a fraudster.

The bank as a financial institution is a complex organisational structure that includes independent organisational units, formally separated by functions. When constructing a model of financial crime, one should also take into account the environment that forms the relationship with customers and any other person. Therefore, when constructing a model, it is necessary to formally identify the place where financial crimes are committed – banks. In addition, the functional composition of persons, the relationship between which and the banks lead to financial crimes. The authors believe that such persons are directly fraudulent and deceiving. It requires attention to highlight the face, which assists. In banking practice related to financial crimes, the formal acquisition of financial resources is mainly carried out in favour of an outsider. Such a person becomes the formal owner of funds and other benefits that were obtained as a result of a financial crime in the bank. Moreover, financial crimes are not carried out by just one person, usually it is a certain group of people who have their roles.

A fraudster is the main manipulator, an organiser who took possession of financial resources, regardless of whether he is their formal owner or not. Fraudsters can be: owners and top management, clients and other persons with whom the bank has financial relations or persons who can influence decisions and the provision/receipt of financial services, decisions and implementation of financial transactions of banks, clients of banks. A defrauded – a person who has lost money as a result of a financial crime in a bank. A bank itself acts as such a person. Turning to the typology of financial crimes in banks, it should be noted that the most common type is when a financial crime is commited as a result of the withdrawal of financial assets from banks. Or such a person is a bank client who has financial relations with him. Assistant - a person who is formally or informally connected with a fraudster and can be involved in any of the stages of financial crimes in the sphere of monetary circulation/financial obligations, who formally receives money, signs documents, assumes responsibility.

The type of financial crime in banks is determined at the design and preparation stage. The financial crime model in banks takes into account the basic characteristics, regardless of the situational characteristics of financial crimes. This allows more fully organising activities aimed at combating financial crimes in banks, as well as, if necessary, focusing on it directly in ensuring the security of the resource base, deposit, credit, foreign exchange and investment activities, the formation and maintenance of a debt portfolio, income generation and implementation of expenses, and, consequently, in banks in general. The presented unified model, in the authors' opinion, can be considered prognostic as well, since it makes it possible to evaluate the information accumulated during the counteraction for the presence of fraudulent manifestations that were not previously identified, as well as on the eve of their implementation or online. However, the detection of financial crimes in banks is an indispensable, but not the only component of preventing/counteracting this negative phenomenon. The relationship between the detection of financial crimes in banks and other elements of a fight, the indispensable accounting of which should significantly reduce the risks of financial crimes, its negative impact on all components and financial security in banks as a whole, is shown in Figure **1**.

In addition to the above, it is legitimate, in the authors' opinion, to talk about the model of organising activities in banks to identify financial crimes, which provides for a clear definition in the process of identifying financial crimes in banks, the functions of its supervisory board and management, authorised to comply with the established procedure for identifying financial crimes of persons, heads of departments/services, as well as employees (Figure **2**), which should have a positive effect on the observance of financial security in general and its individual varieties. Along with this, in large systemically important banks such a separate area of risk management and financial security as fraud management can be created, which will be responsible for coordinating the efforts of all actors involved in detecting financial crimes, effectively contribute to increasing their level of financial security and its individual components.

Consequently, the effectiveness of detecting financial crimes in ensuring financial security will be predetermined by the indispensable use of a unified model of financial crimes in countering it; taking into account the place and role of timely and maximally complete identification of the model of financial crimes in the aggregate of the components of the fight against

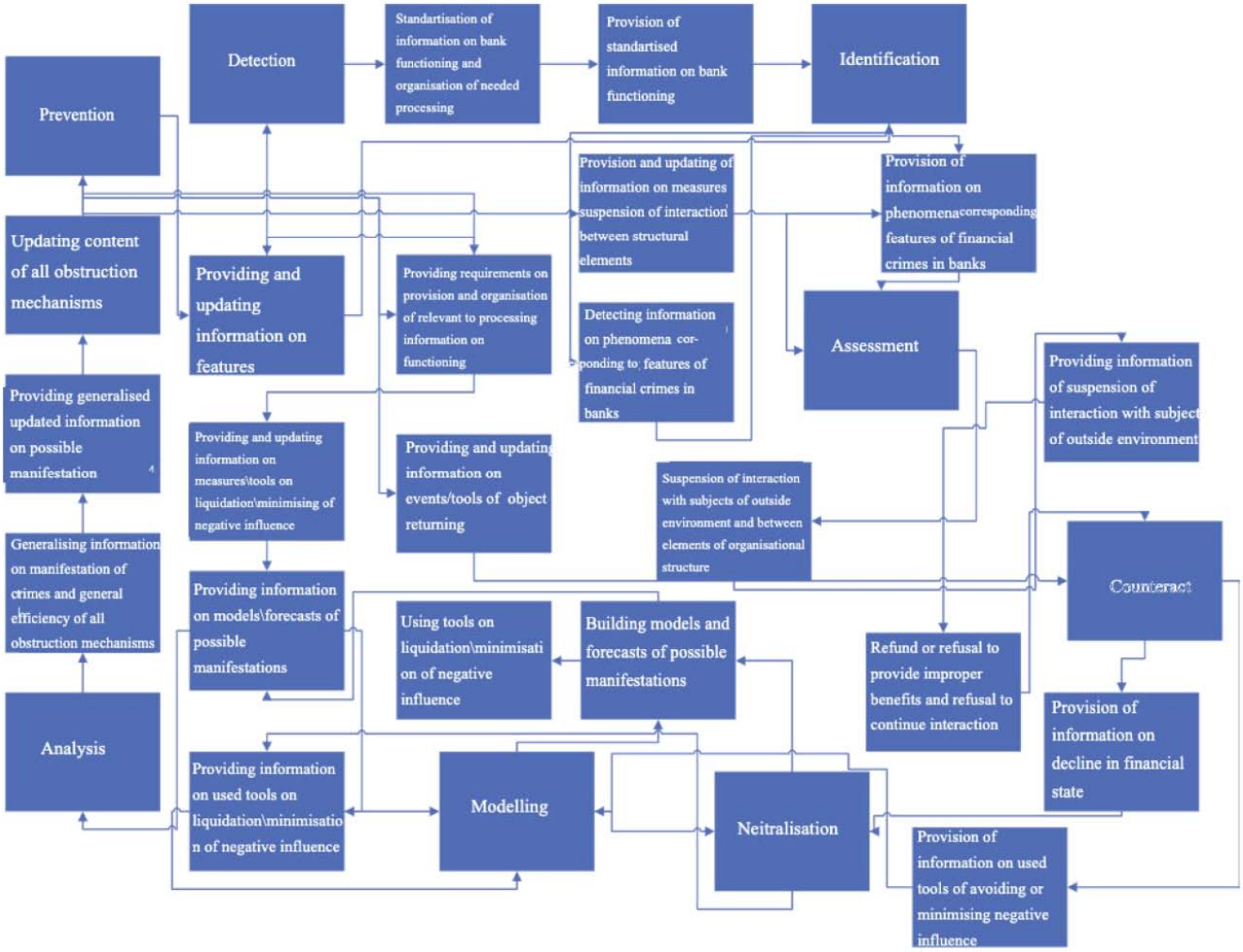

Figure 1: Relationship between the detection of financial crimes in banks and other elements of the fight against it.

this negative phenomenon; clear distribution and effective implementation of the functions of the supervisory board, the board authorised to comply with the established procedure for identifying the model of financial crimes of individuals, heads of structural divisions and services, employees to identify the model of financial crimes.

To promptly detect fraudulent transactions in bank card transactions, neural networks based on the feed-forwar architecture should be used more widely, which take into account the peculiarities of the functioning of the human brain/behaviour model and propagate a signal from inputs to outputs. At the same time, based on the analysis of information about the age, employment and income of s cardholder, the number and frequency, as well as the time of day and place of making large purchases in an automated mode, a conclusion can be made about the legality of the transactions carried out or the presence of transactions that arouse suspicion. This approach will make it possible to increase the effectiveness of compliance control in countering financial crimes, reduce financial losses, and, therefore, will help to increase the level of financial security.

Usually, only a comprehensive accounting of all these areas of a fight against financial crimes, as well as the features of the manifestation of financial crimes in the seizure of financial resources, the transformation of existing financial obligations, its quantitative and qualitative negative impact on the deposit, loan and investment portfolios, currency and debt positions, income and expenses can to a large extent (of course, in combination with other measures to comply with financial security) bring banks closer to achieving the proper level of resource, deposit, credit, investment, debt, currency security, security of income and expenses in particular and their financial security in the whole. At the same time, without diminishing the importance of timely and full-fledged detection of financial crimes in ensuring financial security, it should

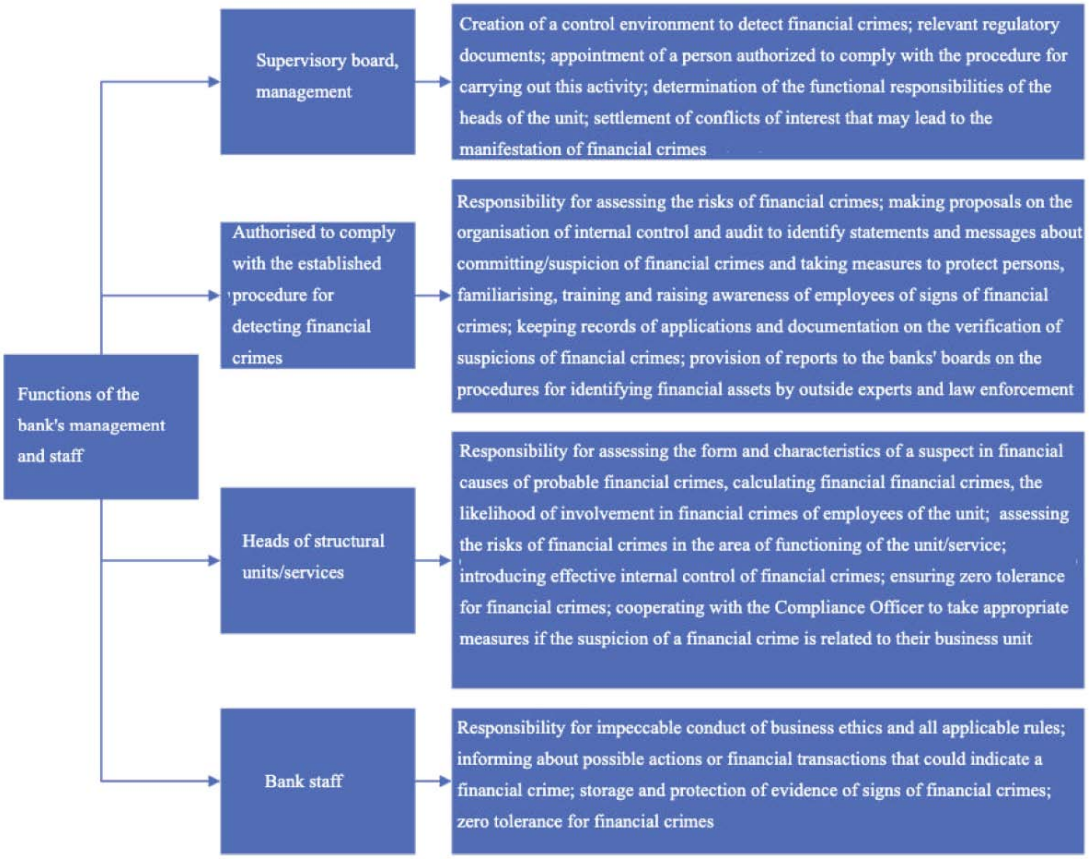

Figure 2: Functions of the bank's management and staff to identify the financial crime pattern.

be noted that, along with this, considerable attention should be paid to improving methods of preventing them in the banking sector in maintaining financial security.

To ensure the financial security of the bank, along with other measures, it is necessary to counter all kinds of manifestations of financial crimes, aimed primarily at preventing them, narrowing the possibilities of their implementation, since the latter is much more effective and efficient than identifying and suppressing already committed crimes. Therefore, in the authors' opinion, it is precisely the prevention of financial crimes in domestic banks at the macro- (national), meso- (banking sector) and microlevels (banks) that should become an imperative for the formation and implementation of measures to counter such manifestations, which will significantly affect the increased level, in particular, resource, deposit, credit, currency, debt, investment security and security of income and expenses in banks and financial security in general.

Research on approaches to detecting and preventing financial crime should be based on the methods used in the investigation of fraud with financial resources and financial obligations by law enforcement agencies, auditors and internal banking services that are used in the practice of banks. Among such approaches (Figure **3**), in the authors' opinion, it is necessary, first of all, to single out a universal one, which can be extended to the fight not only against fraud with financial resources but also against all types of financial crimes, since the latter is only camouflaged for banking operations or services, and the emphasis on them can diminish the effectiveness of detecting financial crimes, determine its wrong direction, and not correctly identify the object of fraud. In general, the activities of banks in the field of combating financial crimes in the field of financial security should be aimed at:

1) Unconditional compliance with the relevant provisions of regulatory legal acts, guidelines and codes of business ethics, internal instructions, rules, standards and procedures for the formation and use of financial resources, compliance with financial obligations;

2) Maximum approximation to the best practice in minimising financial losses, preventing the manifestation of financial crimes;

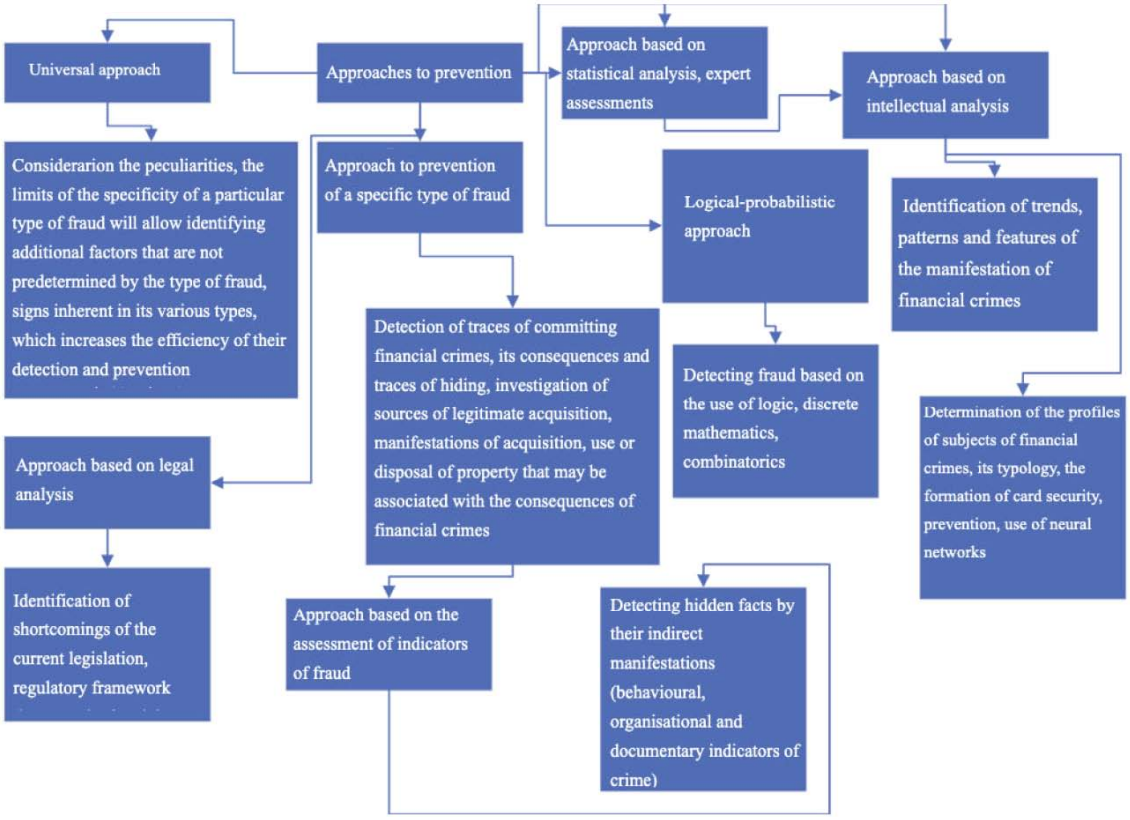

Figure 3: Approaches to preventing financial crime.

3) A dramatic reduction in the level of financial crimes while observing the principle of zero tolerance to them;

4) Raising awareness of owners, top managers, a staff of banks, their clients and counterparties about the signs of financial crimes, their negative financial consequences and methods of their recognition/detection/investigation/prevention/counteraction, minimisation of negative consequences in ensuring financial security;

5) Continuous improvement of financial crime risk management through the continuous collection and analysis of data that may indicate financial crimes, and based on which such risks and the impact of management decisions on the scale of financial losses can be assessed, as well as the inclusion of such risk management in all businesses-processes, and potential risks of financial crimes – in the register of banks' risks and organisation of risk distribution;

6) Improvement of internal control and audit related to the prevention and detection of fraud; joining the efforts of representatives of internal and external audit of banking institutions;

7) Compliance with the anonymity of persons who reported financial crimes;

8) Implementation of timely/due diligence of suspicions of financial crimes in order to avoid/minimise financial losses;

9) Provision of appropriate material, labour, financial and information resources to prevent, detect and investigate cases of fraud.

Such activities should be carried out at all stages of the organisational structure of banks and maximally contribute to increasing the level of financial security. Improving financial security should help to prevent the risks of fraud of those who make management decisions in banks, for which this aspect of banking should be under constant effective banking supervision, the program of which should assess the overall level of corporate governance in banks and their individual subsystems, the level of corporate ethics in them, the presence of risk-oriented management and social responsibility of owners and top managers of banks. At the same time, banking supervisors should know modern methods of financial crimes, the risks of its manifestation, the negative consequences of their implementation, the behavioural models of owners and

top managers, the criteria for their dishonesty and the incentives for the implementation of progressive market strategies that should become indispensable components of stress testing of banks. Both separate indicators of the risks of financial crimes and their integral assessment should be widely used in supervisory activities. In this regard, given the importance of preventing/minimising the negative manifestations of financial crimes on the formation of an appropriate level of financial security, it seems appropriate to create a special group/unit in the structure of the banking supervision department to detect financial crimes/scheme transactions in banks.

Along with this, in order to prevent financial crimes, the subject of increased attention, in the authors' opinion, should be such an important type of financial control as constant effective control over transactions on client accounts, intra-bank movement of funds and reporting (Table **1**).

In this context, in the authors' opinion, it seems advisable to create specialised units/groups of fraud monitoring in banks, improve the internal audit of financial transactions, which would carry out the following functions (Figure **4**). This will improve the quality of risk management in banks, which should have a positive effect on increasing resource, credit, currency, investment, debt security, security of incomes and expenses of banks in particular and financial security in general. Ideally, fraud monitoring in banks should be automated to eliminate the shortcomings of traditional approaches to its conduct (the limited number of analysed financial transactions in a short time, as well as its possible incorrect signals, which, in turn, entails additional time and labour costs for personnel). To prevent fraud with payment cards, which should increase the financial security, as well as their customers, in the authors' opinion, it is necessary to take such measures (Figure **5**).

Prevention of a significant number of frauds with payment cards will be facilitated by the formation of close attention by the controlling services in: errors with entering CVV (in such cases, the bank must find out from a cardholder the reality of a certain operation, and when a cardholder carries out, block and reissue it); incorrect entry of a card number when purchasing goods/services on the Internet; changes in the country of implementation of transactions/one-time withdrawals in different countries (a bank's response should be identical to the situation with CVV); selection of the number of transactions (due to a fraudster's ignorance of the balance of funds on a card account). At the same time, it is necessary to develop measures to protect against interference with the operation of the ATM when performing cash withdrawal operations (leaves the balance of a card account unchanged when a fraudster actually receives cash) and sticking a dispenser (cash dispenser) for a fraudster to take cash that was debited from the legal card account of a card holder.

In addition, the obligation of banks issuing payment/credit cards and processing centres to inform law enforcement agencies about the claims of

Table 1: Control Over Transactions on Client Accounts, Intra-Bank Movement of Funds and Reporting

Type of control	Predestination of control
Control over the withdrawal of funds from client accounts	In the absence of proper control over the movement of funds available on a client's account, money can be unreasonably debited in favour of third parties, causing damage to both banks and its clients
Control over clients' payments based on fraud monitoring	In the absence of such control, the growth of the scale of unauthorised actions with the funds of the bank's clients is restrained, and, consequently, financial losses scale up, undermining the financial security of the bank
Control over the transfer of funds on behalf of a bank	In the absence of proper control, funds from the client's current account are transferred on behalf of the bank to any company with the payment designation, but without supporting documents that are missing/fabricated
Control over the correctness of writing off shortages	In the absence of proper control, it is possible (access to accounting documents) that the write-off, say, by employees of the cash-settlement centre of a bank, the formation of a shortage and its transfer to its other structural divisions, where such an operation can be detected only over time, which makes it possible to confuse traces
Control over the correct allocation of personal expenses	In the absence of proper control, it is possible to manipulate the own records of the bank's accounting department, referring to the client account/account of a shell company created to absorb such expenses
Control over the correctness of reporting	In the absence of proper control, the following are possible: manipulations, falsifications and changes in accounts/documents; hiding information about transactions in accounts/documents; reflection in the accounting of non-existent transactions; deliberate misapplication of accounting policies that results in financial losses

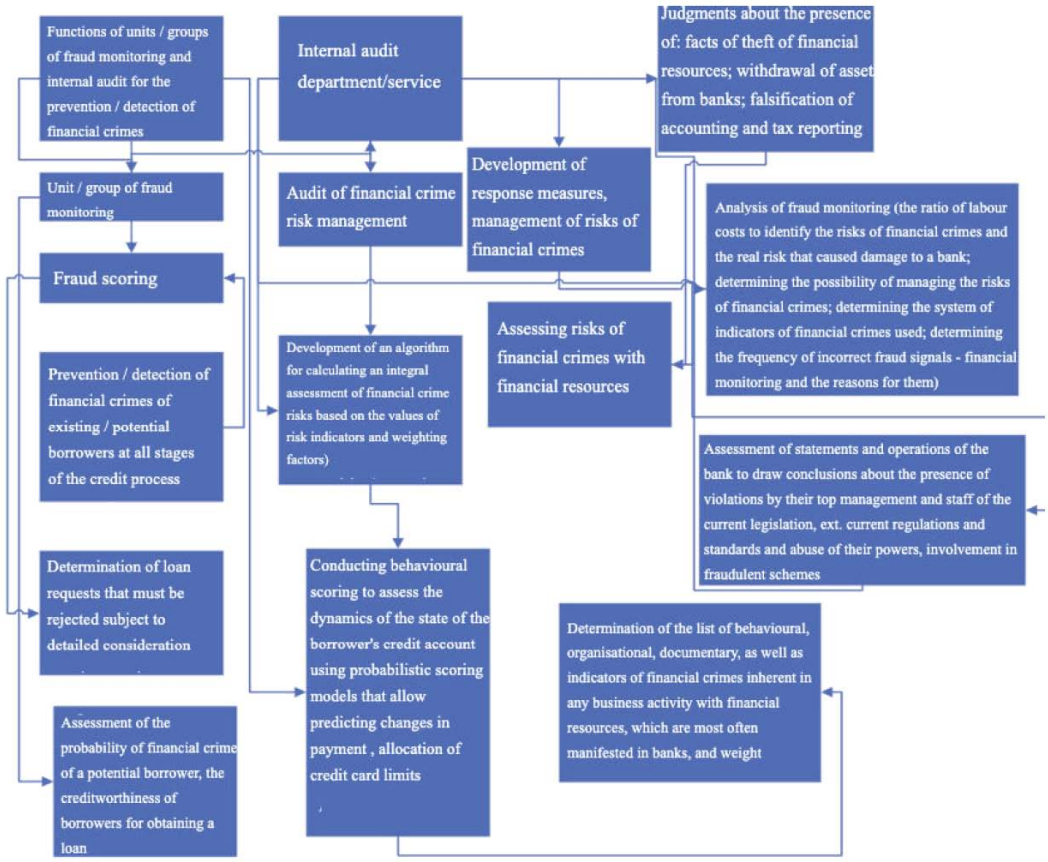

Figure 4: Functions of departments/groups of fraud monitoring and internal audit of banks for the prevention/detection of financial crimes.

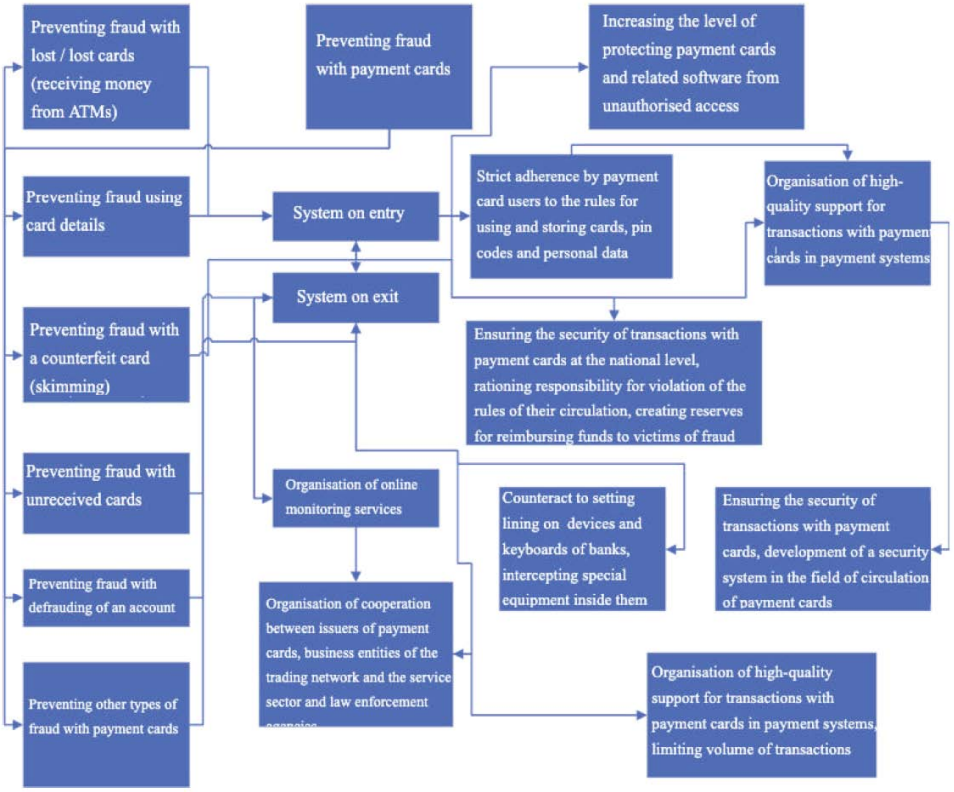

Figure 5: Preventing payment card fraud.

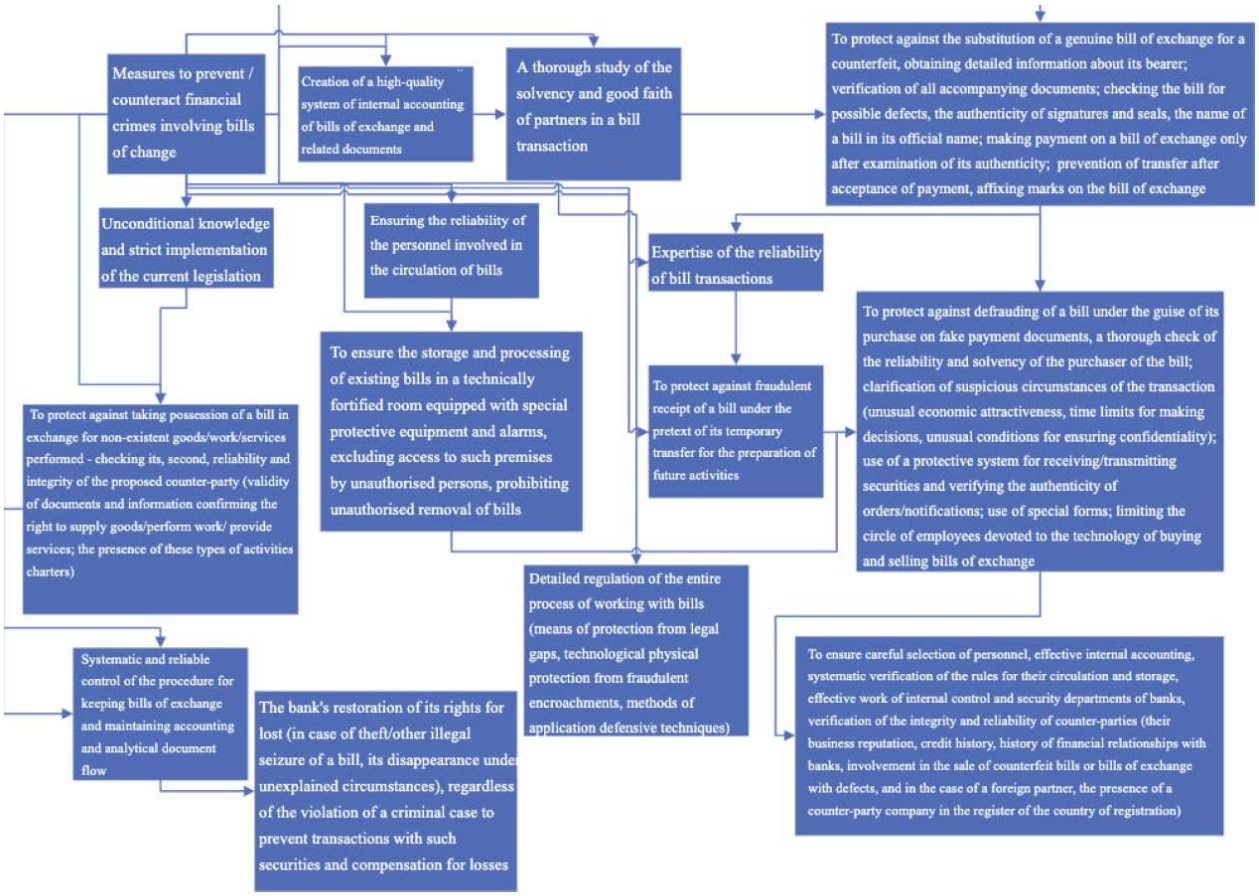

Figure 6: Measures to prevent/counteract financial crimes with bills of exchange.

cardholders, which must be checked regarding possible financial crimes, should be normalised within a short time frame (up to 3 days). The implementation of the aforementioned measures is very important, since card fraud entails voluntary or court-ordered compensation by banks to cardholders for unauthorised funds transferred, and also requires expensive repair/replacement of ATM equipment, which, in turn, negatively affects financial security.

To prevent/counteract financial crimes involving bills of exchange, which negatively affects the security of settlement transactions and the debt security of banks in particular, and financial security in general, such measures should be taken (Figure **6**). Such measures can comprehensively prevent/counteract various fraudulent manifestations in the field of bill circulation with the participation of banks, and, therefore, include: unconditional knowledge and strict implementation of the current legislation; creation of a high-quality system of internal accounting of bills of exchange and related documents; careful study of the solvency, reliability and integrity of the partners in the bill transaction; ensuring the reliability of the personnel involved in the circulation of bills; detailed regulation of the entire process of banks' work with bills of exchange; systematic and reliable control of banks over the procedure for storing bills and maintaining accounting and analytical document flow; examination of the reliability of bill transactions; restoration by banks of their rights on lost bills.

At the same time, special attention should be paid to specific measures to ensure security against theft, substitution of a genuine bill of exchange with a counterfeit one, fraudulent appropriation of bills of exchange, taking possession of a bill under the guise of buying it using fake payment documents, taking possession of a bill in exchange for non-existent goods/work performed/services not provided, fraudulent receipt of a bill under the pretext of its temporary transfer to prepare for the conclusion of a future transaction. In turn, in order to ensure the deposit security of bank customers, and, consequently, the deposit and resource security of the latter, a decrease in the level of which is possible due to fraudulent manipulations, depositors should not agree to re-register the deposit into bonds, savings

certificates and bills, carefully familiarise themselves with bank documents, keep all receipts and expenditures, from time to time demand bank statements.

It is also very necessary to widely introduce into the practice of banks full control over the payment transactions of their clients based on fraud monitoring, which, in addition to personal data on a specific payment, includes an anti-fraud system that contains the profile of the average payer of a certain bank/online store, and also makes possible detection of the country of payment and the issuing bank of the payment card, the size of the payment, the number of payments made from the card/its payment history. At the same time, the appropriate control should be carried out using security filters/comparison of personal data of customers, permitted and prohibited rules for using bank payment cards.

It is very important to maintain an appropriate level of financial security of banks to combat financial crimes as part of combating money laundering with their participation. To prevent financial crimes in the banking sector in ensuring financial security, it is necessary to introduce a full-fledged Big Data technology as soon as possible, that is, methods, approaches and tools for processing large volumes of structured and unstructured data in order to obtain results that a person is able to perceive. This technology makes it possible to clearly classify fraudulent manifestations, test data about them, conduct in-depth and cluster analysis, training in association rules, crowdsourcing (joint problem solving, getting a client-partner), machine learning, and the use of neural networks (Figure **7**).

This technology is applicable for the formation of financial statements; risk management, prevention/counteraction of financial crimes in banks, its forecasting; formation of behavioural models of subjects of financial crimes; segmentation and assessment of the creditworthiness of borrowers; the use of scoring and marketing in banks; assessing the reputation capital of banks in social networks. The use of Big Data protects banks from a decrease in the level of their financial security, since it will contribute to a change in the awareness of business processes, a decrease in the required stages and the number of documents, to introduce automatic determination of the reliability of borrowers, to reduce personnel costs, to use algorithms for the rapid identification of abnormal

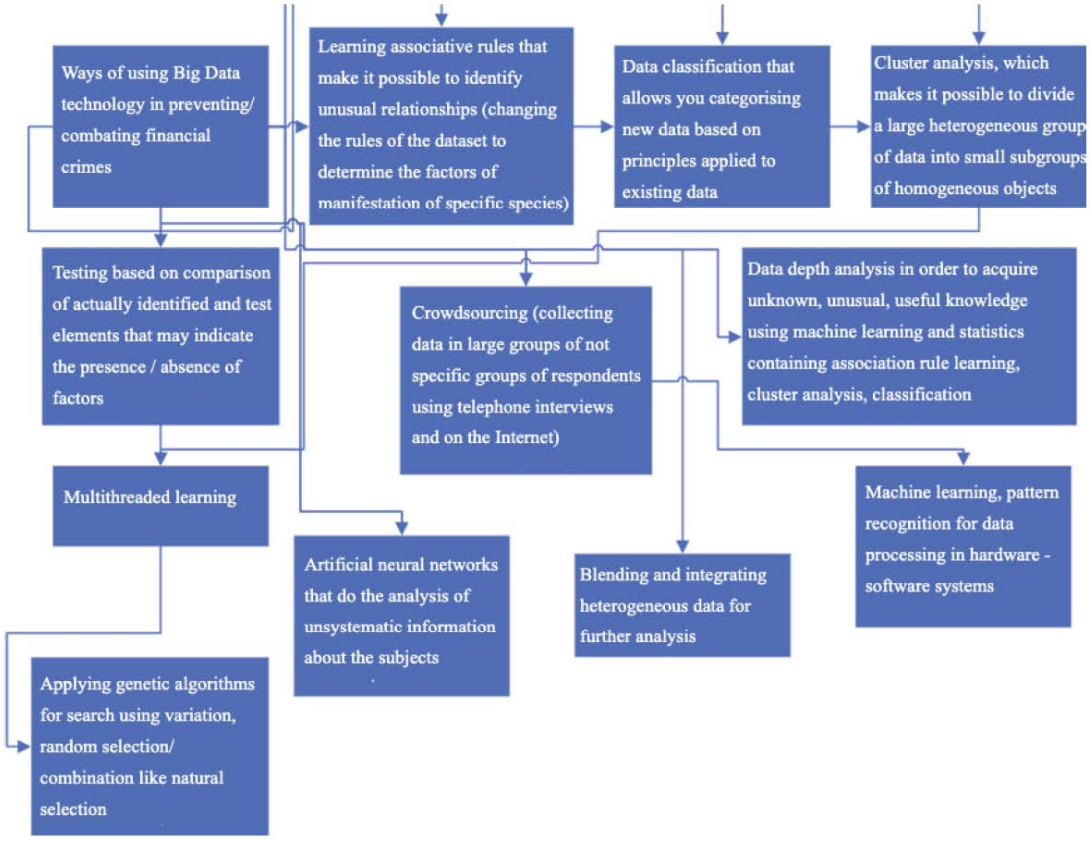

Figure 7: Ways of using Big Data technology to prevent/counteract financial crimes in banks.

activity, and to significantly improve the quality of analysis. and risk management and the possibility of using the blockchain on the principles of distributed storage and processing of transactions, transparency and guaranteed protection allows avoiding intermediaries and verifying the transactions of system participants only by themselves, to obtain reliable information.

To counteract financial crimes in banks in order to increase the level of financial security, it is necessary to develop forensics in every possible way – an independent financial investigation should be carried out in banks, during which evidence of fraudulent activity is obtained, potentially questionable areas of activity/operations /products/transactions are identified, which will further contribute to reducing risks of fraudulent manifestations/improvement of their management practices. Such investigations should involve specialists who have the skills to evaluate accounting documents, financial statements, bank correspondence, financial losses due to misappropriation/waste of assets, as well as operations/sale of banking products/services unfavourable for banks, interviewing bank personnel, customers and counterparties of banks.

CONCLUSIONS

In the authors' opinion, a thorough analysis of law enforcement and judicial practice in considering cases of financial crimes should also contribute to the prevention and detection of financial crimes in banks in order to increase the level of financial security. In particular, heightened scrutiny should be given to the hearings of bank claims against borrowers who, using opaque transactions, have withdrawn assets from debtor companies, thereby leading the latter to bankruptcy. Along with this, banks need to attract highly qualified specialists (lawyers, financial/forensic experts, auditors) to defend their interests in courts.

It is advisable for banks to use the Daily Validation Reports service, which makes it possible to obtain information about clients' activities in the SWIFT system that can be used to independently verify sent/received payment notifications. Clients get access to the reports through authorisation on the www.swift.com website. The reports provide summary analytics on the bank's transaction activities, which allows viewing incoming and outgoing payments in currency, country and counterparty bank. The reports allow a client to see the counterparty banks, senders, recipients and beneficiaries, as well as the total transaction activities of a bank by categories: amount, currency and message type. The data on counterparties will help, if necessary, to interrupt a transaction chain in time. Filters by message type provide the ability to quickly organise the needed data. Each report provides information on daily payments and average volumes (calculated over a 24-month period), as well as a special indicator in percentage ratio, which will quickly identify significant changes in the payment structure. This service will be especially useful for small banks that do not have advanced tools to ensure a prompt response to fraud.

REFERENCES

Aladwan, Zaid. 2020. "Legal basis for the fraud exception in letters of credit under English law ". Journal of Financial Crime. https://doi.org/10.1108/JFC-01-2020-0004

Association of Certified Fraud Examiners: "Who We Are". Retrieved July 6, 2020 (https://www.acfe.com/who-we-are.aspx).

Baker, Richard, Bruno Cohanier and Nancy Leo. 2017. "Breakdowns in internal controls in bank trading information systems: The case of the fraud at Société Générale". International Journal of Accounting Information Systems 26: 20-31. https://doi.org/10.1016/j.accinf.2017.06.002

Chatain, Pierre-Laurent, John McDowell, Cedric Mousset, Paul Allan Schott and Emile van der Does de Willebois. 2009. "Preventing money laundering and terrorist financing: A practical guide for bank supervisors". Washington: World Bank Publications. 304 p. https://doi.org/10.1596/978-0-8213-7912-7

Clinton, Edward. 1996. "Defending banks against consumer fraud claims". Banking Law Journal 113(9): 902-908.

Coogan, John, Elizabeth Forder, Jelena Madir, Norbert Seiler and Clare Wee. 2015. "Combatting fraud and corruption in international development: The global impact of the multilateral development banks' sanctions regimes". Journal of Financial Crime 22(2): 228-241. https://doi.org/10.1108/JFC-10-2014-0045

Diadiushkin, Alexander, Kurt Sandkuhl and Alexandr Maiatin. 2019. "Fraud detection in instant payments as contribution to digitalization in banks". CEUR Workshop Proceedings 2443, 107-117.

Han, Chang-Ryung, Hans Nelen and Matthew Youngho Joo. 2015. "Documentary credit fraud against banks: Analysis of Korean cases". Journal of Money Laundering Control 18(4): 457-474. https://doi.org/10.1108/JMLC-12-2014-0048

Hartmann-Wendels, Thomas, Thomas Mählmann and Tobias Versen. 2009. "Determinants of banks' risk exposure to new account fraud – Evidence from Germany". Journal of Banking and Finance 33(2): 347-357. https://doi.org/10.1016/j.jbankfin.2008.08.005

Hass, Lars Helge, Skralan Vergauwe and Zhifang Zhang. 2019. "State-ownership and bank loan contracting: Evidence from corporate fraud". European Journal of Finance 25(6): 550-567. https://doi.org/10.1080/1351847X.2017.1328454

Higgins, Huong. 2012. "Learning internal controls from a fraud case at bank of China". Issues in Accounting Education 27(4): 1171-1192. https://doi.org/10.2308/iace-50177

Hoffmann, Arvid and Cornelia Birnbrich. 2012. "The impact of fraud prevention on bank-customer relationships: An empirical

investigation in retail banking". International Journal of Bank Marketing 30(5): 390-407. https://doi.org/10.1108/02652321211247435

Hollow, Matthew. 2014. "Money, morals and motives: An exploratory study into why bank managers and employees commit fraud at work". Journal of Financial Crime 21(2), 174-190. https://doi.org/10.1108/JFC-02-2013-0010

International Federation of Accountants (IFAC). 2020. Retrieved July 6, 2020 (https://auditor-sro.org/activity/mfb_ifac/#1).

Li, Zhuolin., Hao Zhang, Mohammad Masum, Hossain Shahriar and Hisham Haddad. 2020. "Cyber fraud prediction with supervised machine learning techniques". In: ACM SE '20: materials of the 2020 ACM Southeast conference (pp. 176-180). New York: Association for Computing Machinery. https://doi.org/10.1145/3374135.3385296

Lokanan, Mark. 2019. "The banks and market manipulation: A financial strain analysis of the libor fraud". Advances in Public Interest Accounting 21: 73-103. https://doi.org/10.1108/S1041-706020190000021004

Nanduri, Jay, Yuting Jia, Anand Oka, John Beaver and Yung-Wen Liu. 2020a. Microsoft uses machine learning and optimization to reduce e-commerce fraud. Interfaces 50(1): 64-79. https://doi.org/10.1287/inte.2019.1017

Nanduri, Jay, Yung-Wen Liu, Kiyoung Yang and Yuting Jia. 2020b. "Ecommerce fraud detection through fraud islands and multi-layer machine learning model". In: K. Arai, S. Kapoor, and R. Bhatia (Eds.), Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing (pp. 556-570). Cham: Springer. https://doi.org/10.1007/978-3-030-39442-4_41

PwC's Global Economic Crime and Fraud Survey 2020: "How can you gain the upper hand?" US edition. 2020. Retrieved June 16, 2020 (https://www.pwc.com/us/en/services/forensics/library/global-economic-fraud-survey-2020.html).

Rahman, Mizanur, Nestor Hernandez, Bogdan Carbunar and Duen Horng Chau. 2018. "Search rank fraud de-anonymization in online systems". In: HT 2018: materials of the 29th ACM conference on hypertext and social media (pp. 174-182). New York: Association for Computing Machinery. https://doi.org/10.1145/3209542.3209555

Stewart, Robert. 2016. "Bank fraud and the macroeconomy". Journal of Operational Risk 11(1): 71-82. https://doi.org/10.21314/JOP.2016.172

The Deloitte Global Millennial Survey 2020. 2020. Retrieved June 15, 2020 (https://www2.deloitte.com/global/en.html?icid=site_selector_global).

Tremblay, Pierre. 1986. "Designing crime: The short life expectancy and the workings of a recent wave of credit card bank frauds". British Journal of Criminology 26(3): 234-253. https://doi.org/10.1093/oxfordjournals.bjc.a047609

Received on 16-10-2020 Accepted on 16-11-2020 Published on 07-12-2020

DOI: https://doi.org/10.6000/1929-4409.2020.09.166