UNIVERSITY OF LJUBLJANA
SCHOOL OF ECONOMICS AND BUSINESS

MASTER THESIS

IMPLEMENTING SAS ANTIFRAUD SYSTEMS AS A WAY TO OPTIMIZE THE PROCESS OF COUNTERING FRAUD IN A FINANCIAL INSTITUTION

Ljubljana, May 2023 ANASTASIIA SUKHAREVA

AUTHORSHIP STATEMENT

The undersigned Anastasiia Sukhareva a student at the University of Ljubljana, School of Economics and Business, (hereafter: SEB LU), author of this written final work of studies with the title Implementing SAS antifraud systems as a way to optimize the process of countering fraud in a financial institution, prepared under supervision of professor Mojca Indihar Štemberger.

DECLARE

1. this written final work of studies to be based on the results of my own research;
2. the printed form of this written final work of studies to be identical to its electronic form;
3. the text of this written final work of studies to be language-edited and technically in adherence with the SEB LU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU's Technical Guidelines for Written Works;
4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;
5. to be aware of the consequences a proven plagiarism charge based on the this written final work could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;
6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;
7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained permission of the Ethics Committee;
8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;
9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;
10. my consent to publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

Ljubljana, May 3rd 2023
(Month in words / Day / Year,
e. g. June 1st, 2012

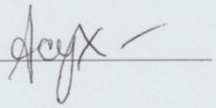
Author's signature: 

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

ABS – (sl. Avtomatizirani bančni sistemi); Automated Banking Systems

AI – (sl. Umetna inteligenca); Artificial Intelligence

ATM – (sl. Bankomat); Automated Teller Machine

BI – (sl. Poslovna inteligenca); Business Intelligence

CDW – (sl. Podjetniški skladiščni sistem); Corporate Data Warehouse

CNP – (sl. Kartica brez prisotnosti); Card-not-Present

CRM – (sl. Upravljanje odnosov s strankami); Customer Relationship Management

EU – (sl. Evropska unija); European Union

FATF – (sl. Finančna akcijska skupina); Financial Action Task Force

FinCERT – (sl. Finančna ekipa za odzivanje na računalniške incidente); Financial Computer Emergency Response Team

JSON – (sl. Zapis JavaScript objektov); JavaScript Object Notation

ML – (sl. Strojno učenje); Machine Learning

POS – (sl. Točka prodaje); Point of Sales

RBS – (sl. Oddaljeni bančni sistemi); Remote Banking Systems

SEPA – (sl. Enotno območje plačil v evrih); Single Euro Payments Area

SQL – (sl. Strukturirano poizvedovalni jezik); Structured Query Language

INTRODUCTION

In the era of progressive development of every aspect of our lives, technology is the key evolving element, being accessible to most people. Today, there is no need to go to grocery stores, clothing stores, theater cash desks, or banks to make a purchase, pay bills, or transfer funds. A person can do all this using his smartphone, computer, or even a watch. The variety of devices that people use and the complexity of the technologies implemented on these devices are also increasing progressively.

Innovations in business are being an essential key for continuing the progress and the economy, enabling some companies getting the competitive advantage over others. According to the Merriam-Webster dictionary, innovations are new ideas, solutions or tools that are used to improve the current business environment and gain a competitive advantage and, as a result, make a profit (Merriam-Webster). Sustainable growth of companies, including banks, is impossible without innovation. Innovations in the banking sector are closely related to the growing digitalization in the global economy. So, for example, from 2000 to 2019, the growth topics of active Internet audience grew by an average of 13.44% (Lukonga, 2018), investments in companies involved in digital products reached a level of more than 118 billion dollars, which is almost twice as much as for 2017 (Young et al., 2018).

One of the main problems for banks is that in recent years competition in the financial market has greatly increased. Working in conditions of enormous competition and changing user preferences forces market participants to try to do something new every day in order to distinguish themselves from competitors and not only maintain, but also increase their customer base. At the moment, the financial sector is developing especially actively in terms of innovation. Technologies that have come from other areas of activity are especially dynamically implemented, such as process automation, deep and machine learning, organizational cultures that are not characteristic of banks, such as agile, and much more. New technologies provide the opportunity to significantly change payment processing, regulatory oversight, risk management, recruitment, new product development, and the way banks interact with their current and future customers, making these processes less demanding of human intervention, making processes more cost-effective, accurate and independent of person. The market has also been significantly affected by the widespread penetration of smartphones, which has opened up a wide range of opportunities for banks to improve the quality of the customer experience for existing customers and attract new ones.

Along with the complication of technologies and their availability, the vulnerability of the digital services used is increasing as well. Under these conditions, frauds are actively operating, including credit and banking spheres. Moreover, given the characteristics of pandemic and post-pandemic time the humanity is experiencing, it is not a surprise that the ways for fraudulent activities are evolving and the number of such cases is growing (Xiaoqian et al., 2021). As an example of different frauds, there can be illustrated cases when

attackers call bank customers, pretending to be real bank employees, and persuade them, for example, to transfer funds to a secure account in order to apparently avoid fraudsters stealing money.

The paper Money Laundering and Terrorism Financing through Digital Payment Systems: A Review of the Literature (Al-Shiha et al., 2018) provides a systematic review of the literature on fraud in banking. The study examines a comprehensive range of research articles, books, and reports published in the field of banking fraud, and identifies several key themes, including types of fraud, causes and effects of fraud, and fraud prevention and detection. As a result, fraud in banking has been shown as a very complicated occurrence. Moreover, several triggers are influencing fraud, which are droven by economic conditions, organizational culture, or technological advancements. The study concludes that there is a need for more research to develop effective fraud prevention and detection strategies, and highlights the importance of collaboration among stakeholders to combat fraud in the banking industry.

Also, the research "Big Data Analytics for Fraud Detection in Banking: A Comprehensive Review" by Bao et al. (2019), provides a comprehensive review of the literature on the use of Big Data and artificial intelligence (AI) to combat financial crimes in the digital age. The study examines a range of research articles and reports published in the field of financial crime and identifies several key themes, including the use of machine learning algorithms to detect fraud, money laundering, and other financial crimes. The findings suggest that AI has the potential to enhance the effectiveness and efficiency of financial crime prevention and detection efforts, by enabling real-time monitoring, pattern recognition, and anomaly detection. However, the study also highlights the need for caution in the use of AI, as it may raise ethical and privacy concerns. The authors suggest that further research is needed to explore the potential benefits and risks of AI in combating financial crimes in the digital age.

As it is stated in the Identity Fraud Study conducted by Javelin (2021), the total amount of stolen clients' funds of US financial institutions in 2020 amounted to 56 billions of USA dollars. Talking about the European statistics, according to the European Central Bank research (2020), losses of customers of financial institutions in the countries of the Single Euro Payments Area (SEPA) in 2019 amounted to 1.87 billions of euro. When it comes to the UK market, the Bottomline Technologies publishes the Treasury Fraud and Controls Research Report (2021), which is a banking fraud report, where states the statistics of 753.9 millions of Great Britain pound sterling. According to the data of the Bank of Russia (2020) the number of fraudulent transactions amounted to more than 775 thousands of rubles, and the total damage from these transactions was more than 10,8 million rubles. There can be detected an increase in the volume of stolen funds compared to year 2019, which amounted to more than 50%. It is worth remarking that these are only official statistics compiled by the Bank of Russia, that were based on reports from credit institutions using customers' complaints. In this regard, the implementation of anti-fraud measures in financial institutions is becoming one of the most important and relevant areas in risk management.

The purpose of this master thesis is to explore the possibilities of SAS anti-fraud systems and suggest how such system can be implemented in the risk management process in a large bank in order to improve and optimize the process of detecting suspicious transactions and help to solve the problems of fraud combating.

The goals of the master thesis are expected to be the following:

- study international nuances of the work of financial institutions as part of the risk management procedures and explore legal practices in this area;
- find and analyze statistics on stolen funds and the most relevant fraud schemes;
- explore a typical process of countering fraud in financial institutions which use information and analytical systems;
- search the most popular anti-fraud systems and compare them in terms of their functionality and technical aspects of implementation and operation;
- conduct a study of the anti-fraud as-is process in a chosen bank;
- identify the weaknesses of the current process to reveal ways for improvements;
- develop requirements for an analytical model that can optimize the anti-fraud process;
- suggest the optimized business process with the use of SAS anti-fraud systems.

The way of conducting this work is built on an interdisciplinary methodology, trying to link both economic, financial, and information disciplines. This study's integrity was ensured by such methods as analysis, comparison, and processes modeling, which made it possible to analyze in detail the process of countering fraud in the chosen bank in order to propose ways for improvement and optimization.

As sources of information, the paper will use both primary and secondary foundations such as regulatory legal acts, materials of scientific papers on the topic of countering fraud, materials of related conferences, as well as materials from the structural unit of the bank, the center for monitoring and responding to computer attacks in the financial sector. Moreover, several bank representatives (whose work is connected with information technology and information security management, investment in technological innovation and partnerships, and oversight of technological risks and cybersecurity management in the bank) will be interviewed.

In order to maintain confidentiality as has been required by the bank representatives, name of the bank and other identifying facts will be altered.

The master thesis will have the following structure:

- Theoretical part that provides an overview of the theoretical and practical aspects of anti-fraud processes in financial institutions, including the legislative and international legal frameworks, current fraud schemes, stolen funds statistics, methods to combat frauds, and comparison of existing anti-fraud information systems.

- Description and analysis of the current anti-fraud process in a large Russian bank, including research on the bank's activity and a description and analysis of the as-is anti-fraud process.
- The main thesis part that focuses on improving the current fraud detecting process through further optimization steps, including the formation and description of an analytical model for using the client's profile in the SAS Antifraud system, as well as an assessment of the expected business effects of the optimized anti-fraud process.
- A review of the research findings and their effects, as well as any possible boundaries, ways for future development, and recommendations for practitioners.
- The summary of the main findings, contributions, and implications of the research, and provides recommendations for future research and practical applications.

1 CHARACTERISTICS OF IMPLEMENTING AN ANTI-FRAUD SYSTEM IN FINANCIAL INSTITUTIONS

The purpose of this chapter is to provide an overview of the theoretical and practical aspects of anti-fraud processes in financial institutions, with a focus on the legislative and international legal frameworks, current fraud schemes, stolen funds statistics, methods to combat frauds, and existing anti-fraud information systems. This chapter explains the classifications of the topic areas and the types of fraud in financial institutions. It also studies the current national and international regulation of the anti-fraud process and frames several issues within it.

According to FinCERT, a Bank of Russia division, 10,797.3 million rubles were stolen by fraudsters in Russia in the 2020 period and there were 775,941 money operations performed without clients' approval. Compared to 2019, this shows a 51% and 33% increase, correspondingly. The number of transactions done through social engineering techniques was nearly 62% of the total transactions made without clients' approval. According to a related law, the funds that have been stolen via these falsified operations cannot be recovered and reimbursed to the affected customers.

In the United States, 56 billion dollars were stolen from customers of financial institutions and 49 million people turned out to be targets of fraud in 2020. That same year, the quantity of stolen funds via social engineering techniques increased by 154% compared to 2019. As it can be concluded from the data on stolen funds from countries in the Single Euro Payments Area, the capacity increase rate of stolen funds grows every year. Based on statistics, the conclusion is that the current measures in place for fraud preventing are not enough.

The parts of this chapter provide a comprehensive understanding of the theoretical and practical aspects of anti-fraud processes and help to set the context for the rest of the thesis.

1.1 Overview of the theoretical aspects of anti-fraud processes in the financial institutions of European Union and the Russian Federation

The report The Future of Banking Risk Management by Härle et al. (2015) describes current trends in relation to risk management in banks, current problems and non-compliance with modern market expectations, as well as observe in detail the processes that need digitalization. Risk functions must cope with the evolution of new types of risk every day, such as cyber, which requires new skills and tools. The authors of the article write about significant changes in risk management in banks that have occurred in the last decade. The global financial crisis outcome resulted in the emergence of numerous rules regarding risk management. Requirements for financing, capital, and liquidity have become stricter, as well as reporting standards in this area. The authors also noticed how attention to the management of non-financial risks has increased. Thus, most of the functions associated with risk in banks are still in the process of being transformed to meet increasing requirements (Härle et al., 2015).

Online stores, banks, and cardholders themselves can suffer from fraudulent transactions. In the event of a leak of card data, attackers try to withdraw the maximum amount of money and leave no traces so that online stores have to deal with banks, who still has to reimburse the lost amount. It is impossible to keep track of cardholders, so an online store cannot know who is on the other side of the screen: an attacker or a respectable client (Jaksic & Marinc, 2019). Therefore, it is becoming extremely important for financial institutions to establish advanced risk management processes.

The survey Protecting the perimeter: The rise of external fraud by PwC (2022) is a report that examines the current state of fraud and economic crime around the world. The survey is based on responses from over 6,000 participants across 114 countries and provides insights into the latest fraud trends and challenges faced by organizations. The report reveals that the prevalence of fraud has increased in recent years, with cybercrime and insider fraud being the most common types of fraud reported. The survey also highlights the impact of COVID-19 on fraud, with remote working arrangements creating new vulnerabilities for fraudsters to exploit. The report emphasizes the need for organizations to adopt a proactive and data-driven approach to fraud prevention and detection, including the use of advanced technologies like artificial intelligence and machine learning. The findings suggest that collaboration among stakeholders, including regulators, law enforcement agencies, and the private sector, is crucial to combat the global threat of fraud and economic crime.

Talking about criminal actions done in the banking sphere, frauds are unauthorized actions intended at thieving a victim's money or gaining access to a victim's property by deception or breach of trust (Ram & Acharya, 2021). As Modi and Dayma (2017) describe, frauds in the banking sector can be divided into several main types:

1. According to the process that is being the object of the fraud:

- transactional: fraud, which is associated with the process of making transactions through various channels (cards, terminals, Internet/mobile banking, etc.);
- credit: fraud, which is associated with the process of working with loans (assessment of the client's creditworthiness, issuing a loan, closing a loan, etc.);

2. According to the composition of fraud participants:

- internal: fraud, which is carried out with the participation of employees of the organization (the Bank);
- external: fraud, which is carried out without the participation of employees of the organization (the Bank).

The syrvey Banking Fraud Survey by SAS (2021) is a report that examines the state of banking fraud across financial institutions in North America. The survey is based on responses from over 200 banking professionals and provides insights into the latest fraud trends and challenges faced by banks. The report reveals that the prevalence of banking fraud has increased in recent years, with phishing, identity theft, and synthetic identity fraud being the most common types of fraud reported. The survey also highlights the impact of COVID-19 on banking fraud, with the pandemic leading to an increase in online banking transactions and subsequently creating new opportunities for fraudsters to exploit. The report emphasizes the importance of adopting a comprehensive and data-driven approach to fraud detection and prevention, including the use of advanced analytics and machine learning technologies. The findings suggest that collaboration among stakeholders, including banks, regulators, and law enforcement agencies, is crucial to combat the persistent problem of banking fraud.

To further study the implementation of these measures, it is necessary to study the legislative regulation of combating fraud at the international level, as well as understanding how it is done in Russia.

1.1.1 Review and analysis of the legislative framework of Russia in the field of fraud control

In 2015, a wave of funds' thefts in the electronic payments area was recorded in the Russian Federation. The result of more than 1000 fraudulent transactions poured out in more than 4 billion rubles of stolen funds. One of the causes of that problem was the shortage of a regulatory framework for controlling and adjusting the fake transactions' monitoring. Moreover, the legally established process for identifying and suspending shady payments did not exist at all. There was also no algorithm for returning money to the legal owner after an unauthorized transaction had been spotted (Votintseva, 2019).

Throughout years, the regulatory framework administrating anti-fraud actions has been significantly refined. Several main documents meant to regulate and control anti-fraud activities have been settled with the Bank of Russia actively participating. Other governing

documents defining the processes in detail have been established as well. It is crucial to understand what are the key moments presented in the regulatory documents, as well as to analyze the legal regulation of anti-fraud actions.

The main changes in Federal Law No. 161-FZ "On the National Payment System", introduced by Law No. 167-FZ dated June 27, 2018, are explaining new concepts of payment system, electronic money issuer, agent accepting payments; expanding the rights of the national payment system; expanding the rules for issuers of electronic money. Key transformations in the Procedures of the Bank of Russia dated June 9, 2012 No. 382-P established the procedure for credit organizations to conduct operations with funds and/or securities in the bank's offices. These changes were introduced to improve the efficiency of the national payment system and ensure its reliability and security.

The order of the Bank of Russia (08.10.2018) specifies the protocol for information exchange between the bank providing services to the payer, the Bank of Russia and the bank providing services to the recipient of funds when the first one detects a transaction without customer authorization. The document explains the end-to-end process of cooperation between the payer's and recipient's banks using the technical set-up provided by the Bank of Russia.

The procedure of exchanging information about the detected suspicious transaction with the Bank of Russia does not suggest a rapid reaction to a detected suspicious transaction in case it has not been suspended by the payer's bank, as the dispatch period for referring warnings to the Bank of Russia is more than one day. The recipient's bank is informed about the detected fraudulent transaction using the Bank of Russia automated system after the finished investigation by the payer's bank, which means there are no ways for the recipient's bank to break off the incoming payment.

The instruction of the Bank of Russia dated December 25, 2018 specifies the process and arrangement of information exchange between the bank providing services to the recipient and the sender of funds, in case of detection of a transaction without customer authorization. Notifications are sent in electronic form, which allows to duplicate the notification on paper. However, this method does not let full reaction to a possible threat online.

Also, in 2018, the Standard of the Bank of Russia was approved, illustrating the processes and format of messaging between information exchange participants and the Bank of Russia in identifying incidents related to violations of information security requirements, including those related to transactions without customer authorization. Such message arrangement supposes a detailed explanation of the JavaScript Object Notation (JSON, which is a lightweight data format that is commonly used for exchanging data between client and server in web applications) scheme for transmitting data about fraud cases. According to the developers, JSON scheme for transmitting data about fraud cases is a standardized format for describing the structure and content of JSON data, which allows for consistent and

reliable communication of fraud-related information between different systems and applications. It can define the required properties, data types, and formats for fraud case data, ensuring the accuracy and completeness of the information exchanged.

At the moment, the used JSON format specified in the standard is out-of-date. Information about the new format is brought to the notice of the information exchange participants through examples of reports on noticed fraudulent operations. There is no particular documented set-up. The problem also arises due to the episodic interaction process updates, for example, not only regarding the JSON format, but also changes in the sequence of the special API requests. Participants of the information exchange have to quickly finalize the processes for generating and sending reports to that API. The described issues hinder the operational process of information exchange and use.

Another regulation dated 17.04.2019 enforces obligations for keeping protection of electronic communications of banks and their clients, client authentication data, and information about banking operations. Additional order of the Bank of Russia (27.09.2018) approved the signs of remittance without customer authorization.

In relation with the process of analyzing transactions, the first two points of the order are screening. It is vital to point out that the arrangement of the Financial Computer Emergency Response Team (FinCERT) database is not described in the manuscripts of the Bank of Russia. The lists that FinCERT presents to the participants of the information exchange can possibly have unproven data about fraudulent operations. As for banks, using such records for online verification (for instance, deferring or declining customer transactions) is relatively dangerous. Mistakenly rejected operations can cause customers' disappointing concern towards the bank. The detection of uncharacteristic client's actions is the most essential and thus complex process.

1.1.2 Overview of the international legal framework in fraud prevention

Within the many-sided cooperation, the Federal Financial Monitoring Service participates in the following international organizations on behalf of the Russian Federation:

- FATF (Financial Action Task Force) on Money Laundering which is a group for the development of financial measures of anti-money laundering. The Russian Federation has been an associate of this group since year 2003.
- MONEYVAL (which is a group of professionals in the field of estimating measures to fight money laundering; they also investigate how terrorism is funded) whose main form of working consists of executing commutual assessment of participating countries based on the 40 FATF Recommendations dated 2012.
- EAG (The Eurasian group) whose role is similar to MONEYVAL.

– Egmont Group which is an international structure that joins together hundred authorities' financial intelligence units. It also enables the participants to get access to a unique private network where users can connect with each other, sharing and interchanging data.

Also, it is vital to mention European Anti-fraud office (called OLAF), whose special activity is to combat fraud with the budgets of European Union (EU). OLAF, being a global law prosecution organization and an independent part of the European Commission, coordinates the activities of specialized p institutions of the EU and competent authorities of the member states in order to fight against fraud with EU funds and budget.

As a result, through the detailed studying of the legislative structures in the field of fraud fighting and preventing, the following basic characteristics and problem areas can be categorized (Curtin & Lazowski, 2019):

– The judicial control of the activities of credit and financial organizations to combat fraudulent activities in Russia is being set up nowadays. A few years ago, the process of fraud operations identification was performed only on the initiative of credit and financial organizations, specifically, banks. Companies and banks decided themselves whether to invest money in the development and application of information systems for transactions monitoring, as well as in hiring anti-fraud specialists for suspicious transactions analysis done manually, or to lose their clients' funds as a result of a not prevented fraud. In this case, there was no protection of the bank's client interests and securities. However, nowadays, the major controlling document is supported by regulatory manuscripts of the Bank of Russia, that hold recommendations how to execute anti-fraud techniques. Moreover, this document explains the process of exchanging information about operations completed with no customer authorization between the Bank of Russia and operators providing services to both payer and receiver.
– On the later of the laws coming into force the anti-fraud strategy became obligatory, but this law does not regulate: the procedure of approving the transaction with the customer; what can be considered confirmation; and how many times during two working days it is required to contact the customer (this is important because if no approval is received from the customer during these two days, the payment is obliged to be fulfilled). The issue here is that keeping the clients' contact database current is an unusual thing demanding great investments. The employees in charge of approving the transaction of a legal body may change often, while the information in the bank's client system is not being actualized. Consequently, a doubtful transaction will be done because of the failure to contact the customer. Also, there is another serious problem in the process of transaction confirmation: nowadays a lot of fraudsters contact bank clients introducing themselves as bank employees. For that reason, the standard method of calling clients back seems to be not sufficient for the transaction confirmation;
– Another problem is the inability to compensate customers for funds in 30 days according to the law, as this time is not enough to perform the analysis. In addition, if a fraudulent

transaction is carried out using methods of social engineering, it becomes impossible to compensate funds, since the customer reveals confidential payment information;

- Russia collaborates with international organizations who control activities to fight fraud and money laundering. The aims of these companies are to develop international guidelines; to share practice and facts about fraud occurrences; and to perform shared inspections of the participating countries' parties for the level of correspondence with the organizations' requirements. The impact done by such independent international organizations is vital, as they force countries to obey the high criteria regarding combating and countering money laundering and fraud.

1.2 Outline of the current fraud schemes in banking sphere

According to research done by Cárdenas et al. (2018) where transactional fraud in the banking sector is analyzed using machine learning techniques, there can be outlined three main channels of transactional frauds: emission, acquiring, and remote banking services. Table 1 below provides examples of banking fraud in these channels.

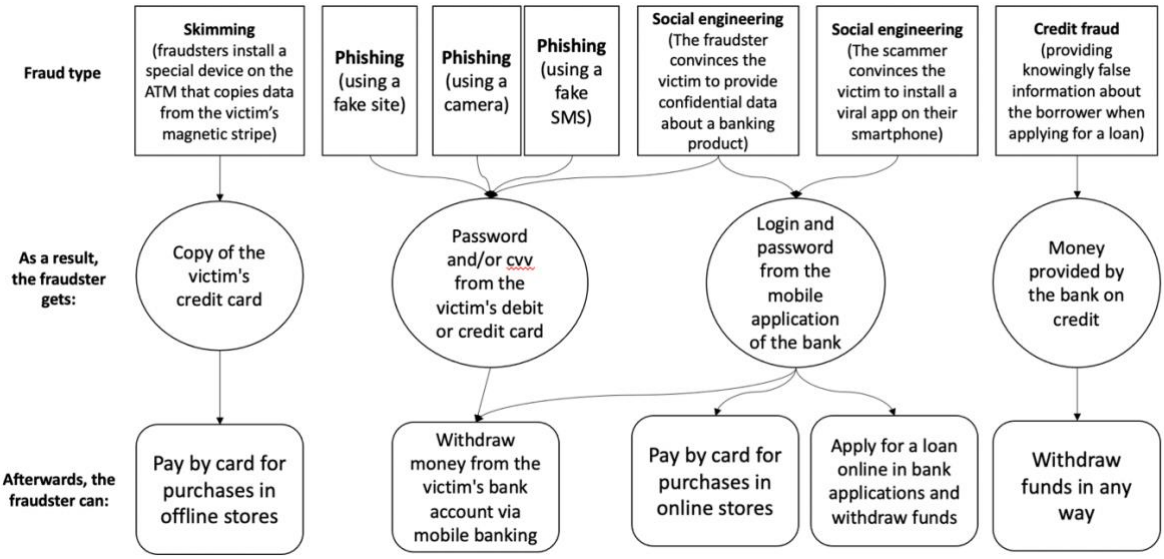
Table 1: Examples of scenarios of banking frauds

Channel	**Fraud characteristics**
Emission	– The client's age is above the threshold value, while this is the first financial operation this client performs; – Two operations from one card are performed in a short period of time from different geographically remote places.
Acquiring	– The process of identifying groups of bank cards for which fraud is carried out in one terminal
Remote banking services	– Requisites for the funds transfer that are not being typical for the client; – Internal fraud: client's remote banking service is connected to a device that belongs to a bank employee.

Source: Cárdenas, et al. (2018).

The problem of fraud in finance area has become pervasive in recent years. With the development of banking products, fraudsters use different fraud schemes, finding vulnerabilities in the products themselves or in the process of using them by customers (Waheedah & Branch, 2021). Types of fraud are shown in Figure 1.

Figure 1: Types of fraud customers



Source: Waheedah and Branch (2021).

The above-mentioned types of fraud are in most cases used in combination with each other, and their split is currently relatively uncertain. Factual operating schemes at different stages include various kinds of fraud.

As an example, let's consider phishing which is one of the most popular fraud cases and is frequently correlated with social engineering. In the research done by Lawson et al. (2020), it has been stated that phishing's main purpose is to obtain confidential data of Internet users by fraudulent means, most often these are credit card data, credentials, passwords. So, attackers use a fake website or fake SMS codes in order to get victim's card CVV or security code so to be able to write off money from the victim's bank account via mobile banking. All phishing attacks are aimed at a person who is the weakest link in any modern security system.

As it has been detected by Alkhalil et al. (2020), targeted and mass attacks through letters using social engineering with attachments, links, and threat letters account for 87% of all types of hacker attacks. Each time there appear increasing numbers on the size of theft as a result of phishing. As it was highlighted in the report, 91% of targeted (and therefore carefully prepared, requiring high qualification) attacks start with phishing, and the average amount of theft in a targeted attack is 90 millions of USA dollars. Reliable statistics regarding the damage caused by phishing attacks to individual users are unknown, but they are quite large, given the number of sites, services and applications that people use in everyday life (Alkhalil et al., 2020). Phishing attack can produce serious consequences: for individuals these includes unauthorized purchases, theft of funds, or detection of theft; for a commercial company a successful phishing attack is likely to result in severe reputational and economic losses.

Attacks of this type are massive, large-scale, and can affect both individual companies and entire industries (Bhardwaj et al., 2020). To implement a high-quality phishing attack, a fraudster needs to create a fake site that is as similar as possible to the real one and the first thing that a person usually sees before going to the site is a link to a web page. Attackers often use subdomains and names of legitimate sites with various typos. Another variant of phishing fraud consists in sending victims links that look indistinguishable from legitimate ones, but actually lead to a phishing page.

The paper Bank Fraud: Types, Detection and Prevention by Bhattacharya and Goswami (2019) provides an overview of bank fraud, including its types, detection, and prevention methods. The study examines various types of bank fraud, such as insider fraud, phishing, and credit card fraud, and identifies several factors contributing to their occurrence, such as weak internal controls and inadequate regulatory oversight. The authors also discuss various detection and prevention techniques, including employee training, customer education, and introducing to the practice progressive tools such as neaural networks, robotics, or intelligent systems. The findings suggest that a combination of these techniques can be effective in detecting and preventing bank fraud. The study concludes that continued research and collaboration among stakeholders are necessary to address the persistent problem of bank fraud.

1.3 Statistics on the stolen funds

Not long ago as a part of their digital transformation, banks started to provide their customers and employees with several different services through the Internet, such as mobile banking applications, an individual account on the bank's website, ability to pay for services using smartphones and so on. Although these possibilities boost the pace and approachability of banking services for clients, they produce extra dangers in the area of information security as well. Since 2018, several projects of the central bank have been initiated to implement the exchange of statistics on detected fraudulent events between the central bank and credit and financial organizations. The projects improved the level of discovery of transactions without customer authorization, and also allowed to collect statistical data on such transactions in Russia for 2019 and 2020.

The following part presents figures on banking operations made without customer authorization during year 2020, and the dynamical pointers' patterns since year 2019. It should be pointed out that the data source for the figures was taken from the FinCERT, which is created using the verified fraud incidents. Should be taken into account that this data may not be 100% exact. First of all, not all clients who have become victims of fraud cases contact the bank to let it know. Then, the process of information exchange between the Central Bank and other banks is still being set up, even though the first controlling documents were released in 2018. As it has been already stated, the interaction configuration is being confirmed by the Bank of Russia regularly, which leads to the banks not having enough time

to settle core procedures. So, it can be noticed that the Bank of Russia is not informed about all the fraud events as they are not reported and thus are not taken into the statistics. However, this study will let to recognize the core tendencies and problems faced by banks and their clients, as well as to figure out what holdups of anti-fraud systems have to be progressed.

1.3.1 Statistical data on thieved funds in Russian Federation

After having studied files and documents of the Bank of Russia's Information Security Department which uncovered operations performed without customer authorization of financial organizations, a summary of statistical data was formed, that can be seen in Table 2.

Table 2: Dynamics of changes in indicators on transactions performed without the consent of the client in 2020 and 2021

Indicator	**2020**	**2021**	**Indicator alteration**
The number of operations done without customer authorization (units)	775941	1035011	33,4%
Individuals	*773008*	*1030860*	*33,9%*
Legal entities	*2933*	*4151*	*41,5%*
The volume of operations done without customer authorization (millions of rubles)	10797,3	13582,3	25,8%
Individuals	*9777,3*	*12131,1*	*24,1%*
Legal entities	*1020*	*1451,2*	*42,2%*
The share of operations done without customer authorization in the total volume of money transfer transactions (%)	0,00120	0,00130	0,0001
Money repaid to clients (millions of rubles)	1104,6	920,5	-16,7%
Money repaid to clients among the total amount of stolen funds (%)	11,30	6,8	-4,5
The total share of operations done without customer authorization performed by means of the schemes of social engineering (%)	61,8	49,4	-12,4

Source: Bank of Russia (2020); Bank of Russia (2021).

The table's last column evaluates the alteration of the indicator in year 2021 compared to year 2020. As it can be seen from the table, transactions performed without customer authorization and their volume raised in 2021 (by 33,8% and 38.8%, correspondingly). The share of transactions performed without customer authorization grew by 0.0013%. It is worth pointing out that this figure does not overdo the target one of 0.005% established by the Bank of Russia. The entire sum of repaid money decreased by 16,7%, and, the share of such funds also decreased by 4,5% compared to 2020. Similar to 2020, the most frequent kind of

fraud in 2021 remained to be social engineering. Also, the share of transactions without authorization performed using social engineering schemes fell by 12,4% in 2021. These progressive dynamics may be associated with the growth of recognition of financial organizations' customers about the procedures for the secure usage of electronic payment instruments, and about the value of financial organizations' collaboration with the Bank of Russia.

It is worth studying statistical data on transactions of individuals in order to come up with a thorough analysis of popular approaches and ways of fraud. Let's examine the indicators regarding the channels used to perform transactions:

- transactions via imprinters, automatic teller machines (ATMs), terminals;
- payment for goods and services on the Internet or card-not-present (CNP) transactions;
- operations in the remote banking systems (RBS).

Table 3 displays statistics on operations done by individuals in years 2020 and 2021 in the regarding the channels used to perform transactions.

Table 3: Data on transactions of individuals for 2020 and 2021 in the context of operation channels

Indicator	**2020**	**2021**	**Indicator alteration**
Aggregated damage (millions of rubles)			
ATMs and terminals (millions of rubles)	740,4	1971,2	**166%**
CNPs (millions of rubles)	4234,4	4140,2	**-2,2%**
RBS (millions of rubles)	3787,8	6019,7	**58,9 %**
The average amount of operation performed without customer authorization			
ATMs and terminals (thousands of rubles)	15,2	23,5	**54%**
CNPs (thousands of rubles)	7,2	5,6	**-22%**
RBS (thousands of rubles)	27,8	29,4	**5,8%**
The number of operations performed without customer authorization			
ATMs and terminals (thousands of rubles)	48,7	83,9	**72%**
CNPs (thousands of rubles)	585,5	742,3	**26,8%**
RBS (thousands of rubles)	136,1	204,6	**50%**

Source: Bank of Russia (2020); Bank of Russia (2021).

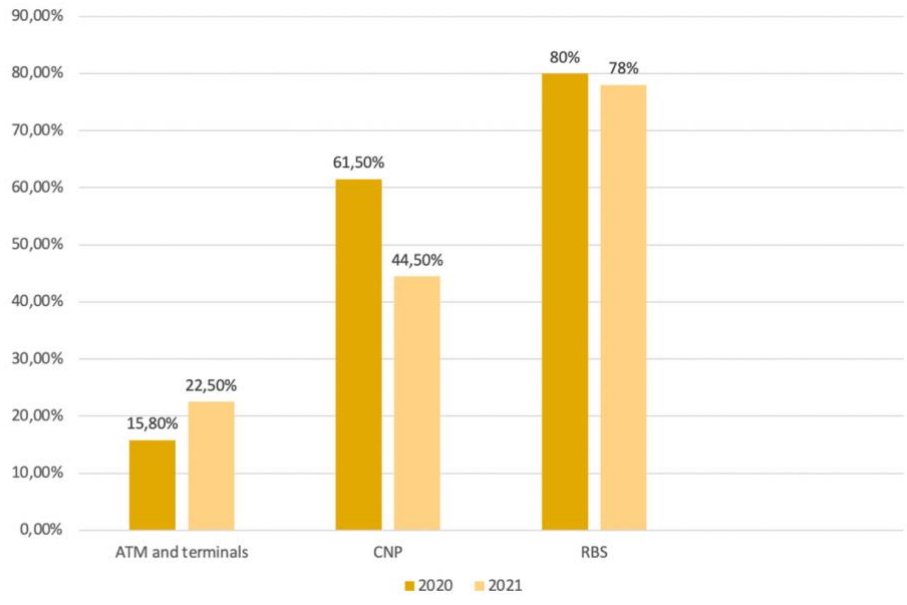
It is worth remarking that people are being significantly vulnerable when using ATMs and terminals: the money loss in 2021 increased by 166% compared to 2020, while the sum of such thefts doubled (from 15,2 thousands of rubles in 2020 to 23,5 thousands of rubles in 2021).

As it can be seen from the table, CNP operations are crucial (4140,2 millions of rubles) as well. Fraudsters frequently use such scheme of money robbing (742,3 thousands of rubles), which makes the maximum cases out of all, but in spite of this, the average amount of such falsified CNP transaction is the smallest (equaling 5.6 thousands of rubles). This fact can be explained: such methods of fraud activities simulate the process for paying for goods and services online, but they cannot enable fraudsters to get access to the customer's banking products.

There is another point to be discussed: the greatest number of damages is caused by RBS operations (equaling 6019,7 millions of rubles), nearly doubling the damage compared to the previous year (6019,7 millions of rubles to 3787,8 respectively). The possibility to entry the customer's RBS allows the fraudster to extract own money of the customer. Moreover, there is the probability of getting and stealing the credit money as well: nowadays, mobile and internet banks permit clients to get credit loans instantly and no signed contract is needed to do that. This appears to become a crucial issue that was caused by the progress of banking products (the fraud scheme implemented in this case is described in section 1.3). Therefore, the amount of fraudulent transactions in the RBS rose by 50%.

Based on the Bank of Russia's research, the prevalent share of fake operations in 2020 and 2021 in all transaction channels accounted for social engineering. Shortly, this is when a victim with his own will transfers money or reveals personal banking data (that allows attackers to steal money) due to the fact of being under great mental and phycological pressure. The current explanations why scammers find social engineering tools easy are discussed in 1.3.

Figure 2: The share of transactions performed without the consent of the client, using social engineering methods



Source: Bank of Russia (2020); Bank of Russia (2021).

The Figure 2 illustrates contribution of social engineering in years 2020 and 2021 in terms of the following transaction channels:

- transactions via imprinters, automatic teller machines (ATMs), terminals;
- payment for goods and services on the Internet or card-not-present (CNP) transactions;
- operations in the remote banking systems (RBS).

As for legal entities or individuals, we also see an increase tendency in the average transaction amount: in 2021, the average amount was 347.8 thousand rubles compared to 152.1 thousand rubles in 2020. The total amount of stolen funds also increased by 46% in 2021. Data on stolen funds of legal entities can be found in Table 4.

Table 4: Data on operations of legal entities for 2020 and 2021

Indicator	**2020**	**2021**	**Indicator alteration**
The number of transactions performed without customer authorization	2933	4151	**41,5%**
The volume of transactions performed without customer authorization (millions of rubles)	1020	1451,2	**42%**
The average amount of one transaction performed without customer authorization on the accounts of legal entities (thousands of rubles)	347,8	349,6	**0,5%**

Source: Bank of Russia (2020); Bank of Russia (2021).

As for legal entities, it can also be pointed out that even though there was nearly no growth tendency in the average transaction amount (0,5%), the quantity of stolen money rose nearly twice (1020 millions of rubles in 2020 versus 1452,1 millions of rubles in 2021), as well as grew the amount of frauds.

1.3.2 Statistics on stolen funds in the United States

According to the research conducted by Javelin (2021), the overall volume of stolen funds of US financial institutions' customers in year 2021 was more than 62 billion US dollars, while the amount of people who were fraud victims was more than 53 million.

The whole amount of stolen funds can be grouped by the scheme of stealing money. For example, the biggest loss of money (nearly 28 billions of dollars) was because of identity fraud scams (this is when fraudsters communicate straight with their victims) which moreover impacted 27 million US people. Important to say, that this type of fraud is much more dangerous than any other because scammers tend to be very cunning physiologists, and victims are artfully conducted to perform any type of required actions to reveal their personal data (even not realizing that something goes wrong). Methods used can be diverse, such as a face-to-face conversation, phone call, text message, or email sent. And also, the

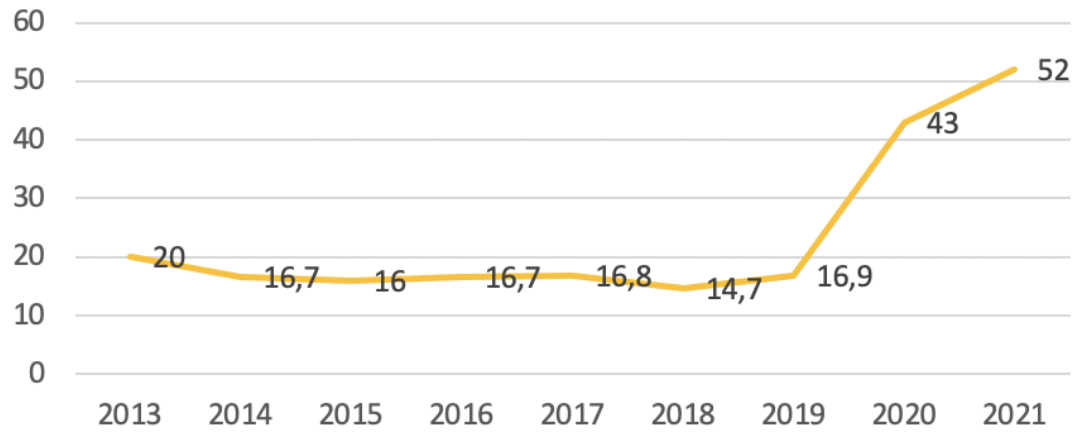
situation background, when a victim gives out this information, is usually "in the right place, in the right time".

However, the traditional identity frauds (when fraudsters use any sort of their victims' personal data to steal money from them) were also significant and impacted 15 millions of people who lost up to 24 billions of dollars.

The situation of identity frauds is worsening, especially because of the COVID-19 pandemic as then most of the people all around the globe were spending a lot of time online and tends in digital behaviors have changed, enabling more new sophisticated fraud schemes to appear.

Summing up, the biggest part of the stolen funds (which was nearly $52 billion) was taken when scammers directly communicated with clients using social engineering techniques. The average sum of a transaction made without customer authorization amounted to $1.1 thousand. Figure 3 illustrates the changing aspects of the stolen money volume using social engineering methods from year 2013 to year 2021.

Figure 3: The volume of stolen funds of US financial institutions' customers using social engineering methods (billions of dollars)



Source: Javelin (2021).

To be more precise, the growth in year 2020 reached 154% in contrast to 2019 (43 billions and 16,9 milliards accordingly) and in year 2021 numbers of losses rose from 43 billions to 52.

1.3.3 Statistics on stolen funds in countries that are part of the Single Euro Payments Area

The latest European Central Bank report (2020) presents statistics on stolen funds of financial organizations' customers in countries of the Single Euro Payments Area (SEPA)

in year 2019 (but was conducted in year 2020). According to it, the overall volume of all transactions done in year 2019 was 5.16 trillion euros (and 4.84 trillion euros in year 2018), and the amount of the stolen funds was 1.87 billion euros (and 1.8 billion euros in year 2018). It is important to point out that the fraudulent transactions' share raised by 13% in comparison to the previous year, while the total volume of all transactions done increased by 6.5%. So, the growth rate of fraud is 2 times greater than the growth rate of the overall transaction volume. The graphic chart that is provided in the report shows the dynamics of stolen funds' volume and their share in the total transaction volume.

As it can be seen from the chart, the CNP transactions and payment for goods and services on the Internet make up the majority of fraudulent operations, and amounted to 80% in year 2019. The portion of such fraudulent transactions rose by 4.3% since year 2018. Important to say that the share of fraudulent operations out of the overall volume of transactions increased in 2019 compared to 2018. This undesirable development means that the protection measures applied seem not to be sufficient. Hence, further fraud-combating methods are needed.

According to OLAF report (2021), cases of fraudulent activities kept on profiteering in year 2021 and fraud schemes themselves developed to more high-level and adjustable intensities. They kept on using diverse fraudulent ways that exist due to the varied operations done worldwide; using constantly developing digital tools in their illegal techniques, thus emerging their criminal business tactics.

The statistics study of the stolen funds concludes the following:

- The growth of the volume of stolen funds in Russian remote banking channels is related to an increase in the average amount of a fraudulent transaction by almost half. This might be as a result of banks issuing credit loans to customers instantly in the mobile applications, and scammers get their advantages of this feature.
- The percentage of fraudulent transactions in Russia amounts to 0.0013% and the figure does not overdo the target value of 0.005% established and set by the Bank of Russia. However, it should be noted that the information used for the calculation is not detailed. As it has been mentioned, not every client who has suffered from fraudulent activity contacts the bank, and the process of collecting information from banks is yet automated and not completely corrected.
- The focus of the research is on the methods used by scammers. In years 2020 and 20201 social engineering is the method used in Russia. This technique is perfect for fraudsters for some logics. First of all, the victim provides confidential information about the bank card or login and password to the remote banking, which means it is problematic to recognize a fraudulent transaction using typical information security tools. Moreover, the stolen money cannot be refunded to customers, as they have given out the confidential data on their own.

– The statistics of stolen money in the United States and Europe shows a significant rise in the volume of stolen funds in years 2019, 2020, and 2021.

Current fraud-combatting measures do not give the looked-for results. Therefore, changes in the tactics of anti-fraud behavior in banks are needed in order to give it more flexibility to the actions of scammers. To know what conditions are needed to be increased for preventing the percentage of fraud, it is vital to figure out the existing approaches of scammers. In the following part, current fraudulent methods will be reviewed and ways to combat them will be studied.

1.4 Description of the current methods to combat frauds

Before forming requirements for different anti-fraud systems, it is crucial to differentiate what types of threats to people and financial institutions' funds exist, so to understand what these systems should protect them from. To combat fraud in financial institutions, special measures are implemented as part of the risk management policy. As an example, Karpoff et al. (2020) specifies data mining to be the most widely used method in the banking sector in the field of fraud detection.

The ability to detect fraudulent activity is a growing concern for many companies, and more and more fraudulent activity is detected and stopped with the help of data mining. Also, using machine learning, deep learning, and artificial intelligence, banks can solve a number of problems concerning identifying suspicious transactions such as identity substitution, theft of personal account or card data, fraud using social engineering. Machine learning and deep learning are able to recognize fake signatures with higher accuracy than a responsible employee in a bank does, and the algorithm can also detect a non-typical transaction much faster and more accurately than a person, so advanced analytics is successfully used here too (West & Bhattacharya, 2016). So, the modern schemes implemented by fraudsters will be analyzed, as well as weaknesses in the process of using various banking products (letting swindlers to successfully steal money) will be studied.

Information about typical patterns of behavior of fraudsters was formed using the materials of the research paper by Dorn et al. (2021). Based on this evaluation, it will be possible to form requirements that modern anti-fraud systems must meet to cope with identified bottlenecks. The paper examines the typical patterns of behavior of fraudsters in the financial services industry. The study analyzes data from financial institutions in Europe and identifies several common patterns of fraudulent behavior, including repeated attempts at fraud, targeting of specific products or services, and manipulation of customer data. The study also highlights the importance of early detection and prevention of fraud through the use of advanced analytics and machine learning techniques. The authors recommend that financial institutions prioritize fraud prevention and adopt a proactive approach to detecting and mitigating fraud risks.

As it has been explained, falsified methods usually combine multi-type forms. For example, phishing can be implemented at a certain phase using social engineering. Below, the current schemes are listed.

- the "Investor": the scammer phones the bank's client claiming to be an employee of an investment firm and suggests to invest the client's money in cryptocurrency or shares of this firm straight from the account of the client. To perform the operation, the scammer explains that the client has to say the code he receives in the SMS. As stated by the authors, this method is frequently applied to retired people, or on the clients who showed interest in the investments or cryptocurrency before;
- the "Lifeguard": the scammer claims to be an employee of the information security department and requests authorization of the client's operation, which the client obviously did not initiate. The client denies making this transaction. In order to “save” the client’s funds, the scammer immediately offers to confirm the client. To do so, again, the scammer asks the client to tell him the code from SMS;
- the "Loan repayment": the scammer calls the customer claiming to be a bank employee in order to get a so-called loan request confirmation. The client informs that he had not requested any loans. The caller then says that almost certainly the request was created by scammers, and suggests transferring all the money from the current client account to a secure one so to protect the funds. The client shifts the money to the scammer's account.
- the "Remote management": the intruder gets in touch with the client claiming to be a worker from a bank. He insists on installing an application for remote access on the client’s mobile device using different excuses, for instance, to stop or avoid potential risks to the funds. Having got the remote access to the client’s account, the scammer withdraws the money. This scheme has something in common with the "Lifeguard" one, as when the customer does not approve the operation, the scammer offers to install a special software on the device, which (as promised by the fraudster) will not allow intruders to perform any operations further on;
- the "Tokenization of dropper cards": the fraudster phones the client and persuades him to perform the card tokenization in the electronic wallet claiming that it is a safe and protected account. The customer transfers the money to this "secure” account losing it, while the scammer cashes the money.
- the "SIM card capture": the intruder obtains a copy of the client’s SIM card and begins the procedure for restoring access to the mobile banking app account. After getting access to the account, the money is withdrawn.
- the "Refusal of signed contracts": the intruder approves the loan issue in the mobile app, cashes the borrowed funds or transfers them to another account. Afterwards, he goes to the bank or even contacts the police saying that he did not confirm the loan, but scammers did that, thus asking for the refund;
- in year 2020, using the COVID-19 pandemic backgrounds, fraudsters executed methods involving false repayment for harm caused by the coronavirus. For example, mailings

with links to phishing websites offering to sell masks, disposable gloves, tests, or disinfectants were sent to legal entities.

Using these facts, several major problems can be distinguished:

- Nearly every method applies a social engineering component. For instance, fraudsters profit from the fact that clients possess a little knowledge concerning banking products. The customer is made to perform the operation on his own under the pressure of transferring the savings to a protected account. This social engineering approach is significant for fraudsters because the transaction is performed by the client himself. Also, obviously, it is hopeless for the client to get the money back.
- Mostly in all the cases fraudsters get in touch with the client by the phone. As it is stated by the Bank of Russia, in year 2020 the share of mobile phones fraud has spread: most fraud calls are automated, and clients are reached by robots. There can be performed enormous number of fraudulent calls daily and the most calls are done with the real number replacements. Consequently, the method of calling the client back to get the approval for the transaction is at this time insufficient, as clients do not believe that they get the real call from the real bank representatives and not the fraudster.
- The volume of credit frauds is expanding. The possibility of an easy credit obtainment in mobile and online banking provides fraudsters possibilities for a significant capitalization as they can perform defrauds with all people, not focusing only on the wealthy.
- It is not enough to fraud-verify a single transaction. Online verification should use all possible various channels, such as information from the bank's system for client service (cards release procedures or clients' complaints), or personal data about the client (the age, address, working history, bank history, place of work, etc.).

There could be developed several potential tactics to resolve the above listed difficulties. Firstly, the most apparent and straightforward way seems to be the raising and improving the level of customers' awareness about the banking products, their possibilities and usage. Earlier, it was assumed that only adult people become the victims of social engineering tricks (as they seemed to be the ones who rarely used mobile applications). However, during the Antifraud Russia 2020 conference, it was reported that the average age of social engineering victims had lowered, meaning that younger people also get caught by fraudster actions. It might be because they are nowadays active users of convenient banking products and might misjudge their degree of technical competence, thus inadvertently becoming victims of social engineering. Consequently, it is obligatory to deliver information to clients regarding the secure money-behavior using diverse means of reaching the clients. For instance, brief corresponding material should be presented to clients in mobile and Internet banks or on the terminals' screens. Besides, during the visits to banks, bank workers should update customers about potential dangers and explain the ways of keeping away from them. Secondly, as a result of the social engineering increase, it is crucial to improve the process of fraud recognition in RBS channels.

The research done by Zhou et al., (2021) provides a comprehensive review of social engineering and its impact on information security. Authors identify various markers of social engineering. So, using the information obtained from the paper, below are several markers of social engineering characteristics:

- the unusual way for the client to type his login and password when logging into the mobile application. For instance, the client typically enters the login/password manually or uses the copy-paste function;
- the turning of VPN in the current session in case the customer has never used it previously;
- various tries to type in the second authentication factor (the fraudster can mishear the code that the victim said, which leads to numerous codes entering attempts);
- uncommon for the client behavior. For example, when the user constantly activates the page and exits it during a quick session, which can be explained that the fraudster is checking the information previously received from the client.

These approaches do not refer to the verification of an exact transaction. Instead, they embrace data concerning the standard client's behavior. Fraudsters' techniques are progressing so quickly that unfortunately the antifraud systems of banks cannot adjust to them in time. Consequently, the ability to quickly change the logic of checking operations is more important for information systems than the complication of arranged guidelines. A user-friendly and adjustable interface of development is required so that prompt modifications could be done and that the bank's security or antifraud department workers could make changes without engaging a special consulting company. Additional feature defining the consistency of the antifraud system is the adoption of knowledge about usual customer behavior (cases of signs that can be studied have been discussed previously).

As it is proposed in the research paper, a machine learning-based approach for detecting fraudulent online banking transactions can be a success. The study utilizes various artificial neural networks processes to evaluate transaction data and recognize specific fraudalent behaviour. The results of the experiments conducted indicate that the proposed approach can accurately identify fraudulent transactions with high precision and recall rates, demonstrating its potential to enhance the security and reliability of online banking systems (Binwahlan et al., 2018).

The research done by Jung et al. (2014) presents a study on current fraudulent schemes and the proposed solutions for anti-fraud systems. The authors reviewed various fraud cases and analyzed the common patterns and characteristics of fraudulent schemes. Based on the analysis, they proposed several solutions for anti-fraud systems, including data mining techniques, fraud risk management systems, and user authentication methods. The paper also discusses the requirements for anti-fraud systems to implement these solutions effectively. The study provides useful insights for financial institutions and anti-fraud solution providers to develop effective countermeasures against fraudulent activities.

Another important research done by Gallo et al. (2021) aims to provide an overview of current fraudulent schemes in the banking sector and to identify detection and prevention strategies that can be employed by banks to mitigate the risks associated with these schemes. The paper reviews the literature on banking fraud and presents a case study of a real-life fraud incident in the Italian banking sector. The paper identifies several types of fraudulent schemes, including payment fraud, identity theft, phishing, and money laundering. Detection strategies, such as data analytics and artificial intelligence, are discussed, as well as prevention strategies such as employee training and regulatory compliance. The paper concludes by emphasizing the importance of a multi-layered approach to fraud prevention that incorporates both technological and human elements.

The paper written by Kassem et al. (2021) presents a systematic literature review of fraud detection and prevention techniques in the banking industry. They have reviewed 58 articles published between 2014 and 2019 and identified various techniques for detecting and preventing fraud, including data mining, machine learning, and artificial intelligence. The paper also detects the importance of employee training and customer education in preventing fraud. The research highlights the need for a comprehensive approach to fraud detection and prevention that includes both technological and human elements.

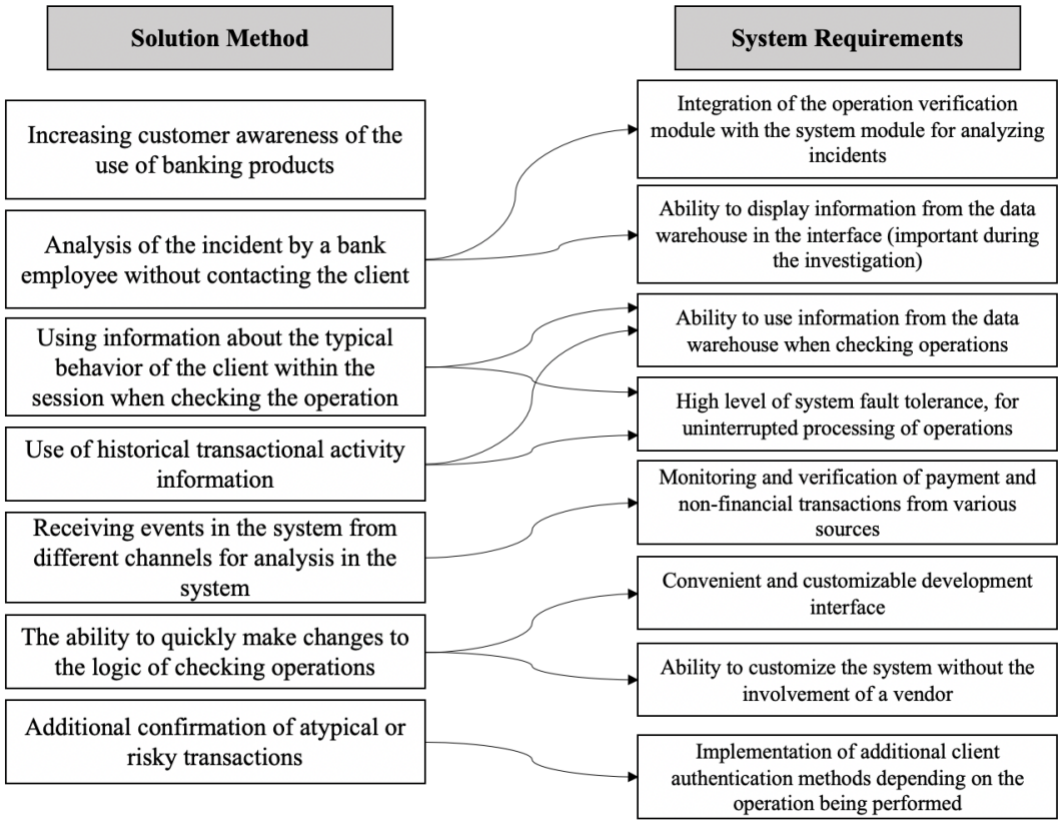
The figure 4 presents the difficulties highlighted by the study of literature of current fraud patterns (Gallo et al., 2021), the suggested solutions to the identified issues, and the requirements needed for an anti-fraud system to be able to apply these solutions (Kassem et al., 2021).

Figure 4: The difficulties of current fraud patterns; suggested solutions

Problem	Solution Method
Increasing frequency of social engineering cases	• Increasing customer awareness of the use of banking products • Analysis of the incident by a bank employee without contacting the client • Using information about the typical behavior of the client within the session when checking the operation • Use of historical transactional activity information
Increasing number of telephone frauds	• Increasing customer awareness of the use of banking products • Receiving events in the system from different channels for analysis in the system
High speed of emergence of new relevant fraudulent schemes	• Using information about the typical behavior of the client within the session when checking the operation • Use of historical transactional activity information • Receiving events in the system from different channels for analysis in the system • The ability to quickly make changes to the logic of checking operations
Availability of obtaining loans in mobile and Internet banking by fraudsters	• Additional confirmation of atypical or risky transactions

Sources: Gallo, et al. (2021); Kassem, et al. (2021).

Figure 5: The suggested solutions of current fraud patterns & their requirements



Sources: Gallo, et al. (2021); Kassem, et al. (2021).

In the further sections of the thesis more thorough fundamental requirements for modern anti-fraud systems will be analyzed in view of the blockages classified in this part. Also, a comparative evaluation of antifraud systems created using these requirements will be presented.

1.5 Explanation of the anti-fraud process in a bank

Countering fraud in a financial institution is an essential measure of risk management strategy (Xue et al., 2021). The risk of higher fraudsters attacks is caused by the accessibility and convenience of the process of using different banking products for clients, thus revealing their vulnerability. There are several directions of anti-fraud operational work in banks (Xue et al., 2021):

- countering transactional fraud;
- combating internal fraud;
- collaboration with regulators regarding the mutual information sharing about operations made without customer authentication;

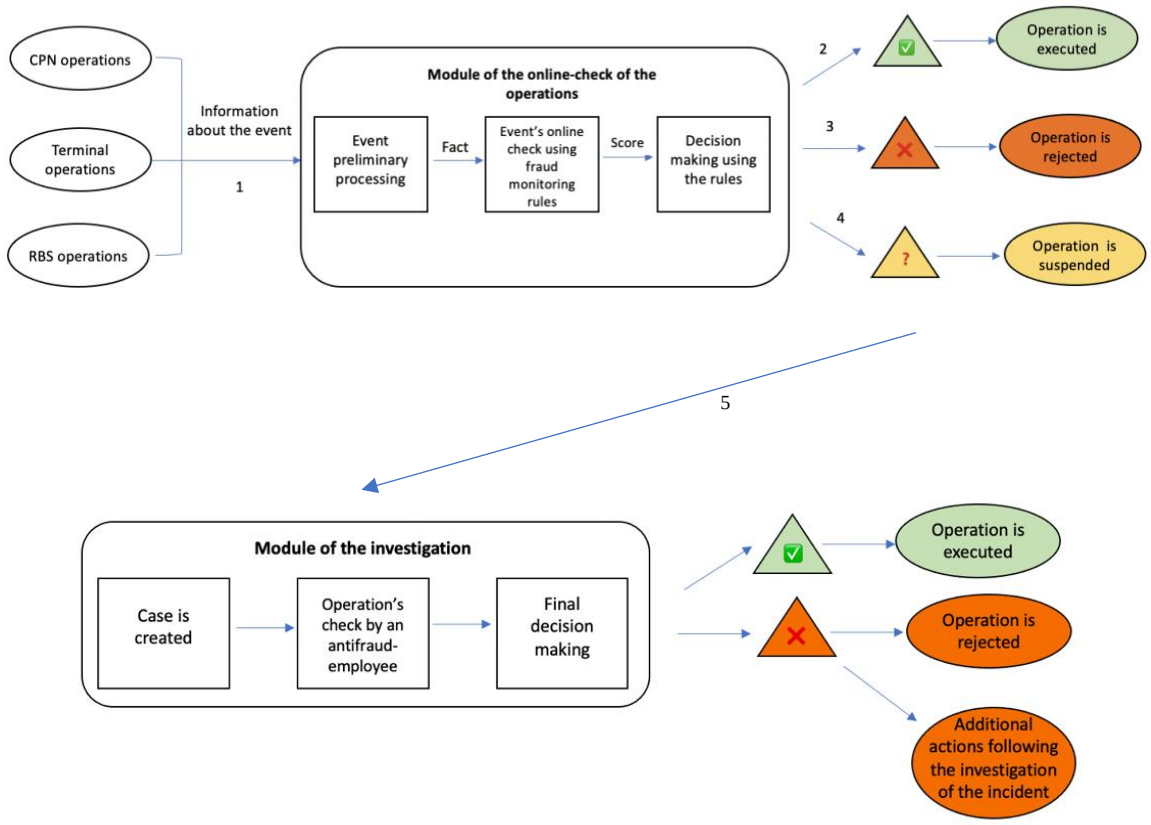
– area of information security.

Let's discuss the key characteristics of these directions implementing and executing in credit and financial institutions.

1.5.1 The process of countering transactional fraud

If the bank aims at preventing fraudulent transactions, there must be implemented a special instrument that enable to examine operations online in real time and to investigate uncertain incidents. To do that, information systems with an online and offline analysis unit for inspecting potential fraud incidents are applied in banks. Based on the report of Gamage et al. (2019) about the process of countering transaction fraud a simplified chart was created (figure 5).

Figure 6: The process of countering transaction fraud



Source: Gamage, et al. (2019).

The client performs a transaction at a terminal, RBS, or via Internet payment. In this situation, data concerning this event is directed to the bank's antifraud system (arrow 1 in the picture). The event is examined along with the anti-fraud rules that were created beforehand. Such rules can be of different kinds (Bialek et al., 2020):

- examining whether transaction or customer details existed in the records;
- examining whether the client's performance pattern is similar to any acknowledged fraudulent methods;
- examining whether the current transaction is similar to the usual client performance pattern, e.g., standard transaction sum, accounts to which the client transforms the money, or devices used to perform transactions.
  The outcome of such transaction inspection by the antifraud system is usually a number of points that indicate the probability of fraud.

  If the points overdo a predetermined limit, meaning that the transaction is outlined as a false one, the following can be done (Bialek et al., 2020):
- the transaction with low or zero points (2) is allowed. The consistent signal is sent to the bank's system of processing transactions and the transaction is executed;
- the operation with the number of points that exceed the limit (3) is disallowed. The transaction is forbidden in the bank system as fraudulent;
- the operation is suspended (4) and the investigation is carried out. If according to the outcomes of the online transaction authentication further examination is required, the material about this operation is forwarded to the manual verification system (5). There an investigation is made automatically and the antifraud employee conducts the operation's verification check manually consuming the client's historical data, aspects of the current procedure, or even contacting the customer in order to get the approval. Next, the operation gets the concluding judgement and it is either confirmed (6) or rejected (7). If it is rejected, there may follow additional events, such as the card blockage or RBS access denying (8).

1.5.2 The process of combating internal fraud

Internal fraud cannot be performed without the bank employees' involvement. Nevertheless, their participations can be both intended or accidental (Ullah & Nadeem Akhtar, 2021). Accidental actions include ordinary employees being not careful enough when using the bank's clients' personal information or loosing individual passwords. Examples of deliberate actions can be when the employee issues unsecured credit because he or she machinates with a fraudster, or transfers money to accounts available to him or her. People cooperate with the bank's internal environment; thus, there is a strong need for their performance control which should be as careful as the control of clients' behavior. This could be realized by monitoring the employees' actions on the continuing basis (Walters & Merwe, 2019). These control actions may be implemented (Hussain et al., 2020):

- Detecting differences of the employee's regular work. For instance, he or she generally sorts out 200 loan applications, but on one day processed 300. In this case, there may be a need for an in-depth investigation into the employee's work. Furthermore, it is essential to react to such unusual activities without delay.

- Applying material guard resources such as cameras, special badges, alarms.
- Limiting employees' access to secure information in compliance with their rank, which means establishing a precise role model in information systems.

The process of collaboration with regulators (Bank of Russia)

In compliance with the conventions implemented in years 2018 and 2019, most of the Russian banks are obliged to share information with the Bank of Russia via the automated system ASOE FinCERT. In order to successfully execute these steps (envisaged by the Bank of Russia), the financial institution has to give quite a lot of resources:

- inclusion in the anti-fraud system of processes for interaction with the Bank of Russia: sending reports on detected transactions performed without the consent of the client, using FinCERT feed lists to verify transactions, sending notifications about detected fraudulent transactions;
- sending notifications to the bank serving the recipient of funds, when a fraudulent transaction is detected;
- continuous monitoring of updates to the process of interaction with the Bank of Russia and updating internal processes in accordance with the updates.

Implementation of information security measures

At the moment, one of the most severe problems regarding information security in bank systems is data leaking, since clients' personal data is easily becoming the initial vector for phishing attacks and social engineering (Chang et al., 2019). Causes explaining that are because of the mistakes of employees and because of technical characteristics of storage and usage of data. The first cause is connected with the aim of preventing the internal fraud. As for the technical causes leading to information leaks, they are connected to (Bhargava et al., 2019):

- using open-source products for arranging anti-fraud systems in test environments;
- running real (and not test) data on test environments with the lack of security policies or data protection tools;
- difficulties in understanding where confidential data is stored and of what types.

Data masking instruments might be helpful in reducing the possibilities and risks of confidential information leaks (Haldorai et al., 2021). To employ them, it is first needed to detect confidential data, and secondly, apply masking tools. Important to note, that the step of masking tools application must be followed by keeping the integrity, configuration and fullness of the data. Therefore, the masked data appears to be synthetic, however, can still be used on test environments (Haldorai et al., 2021).

In order to protect information from leaking, several kinds of data masking techniques can be applied, for example (Jayaprakash & Vetrivelan, 2019):

- static masking: this is an irreversible process of replacing confidential data with realistic artificial one which was created using rules that were arranged beforehand. The data is changed in the only one way, meaning that the primary values cannot be recovered or rebuilt, meaning that static masking technique is appropriate in test environments only.
- dynamic masking: this is a process of replacing data in real time when retrieving the database. This technique can be used equally in test and production environments, for instance, to limit access to data for certain groups of users.

So, this part studied the core points of countering fraud in banks. As a summary, it should be pointed out that all directions demand the allocation of an enormous volume of both financial and human resources, and all are vital. As an illustration, not paying enough attention to internal fraud prevention actions can greatly reduce the effort of a powerful anti-fraud system used to combat transactional frauds. Understanding it, it can be summarized that only the equal improvement of all directions can enable a strong anti-fraud protection mechanism in a financial institution.

1.6 Overview and comparison of existing anti-fraud software

Despite the number of different ways to combat frauds, in this master thesis one of the most successful methods of "antifraud class systems" will be analyzed. These systems are one of the examples of security processes, designed to reduce the level of fraud in banking transactions by timely detecting fraudulent actions. Antifraud is a system designed to observe and stop fraudulent transactions. It assesses each payment in real-time, subjecting them to multiple filters, sometimes ranging in the dozens or hundreds. Anti-fraud mechanisms function by examining payments to determine if there are any abnormalities or anomalies present. The system's purpose is to scrutinize each transaction, identify any instances that appear questionable or doubtful, and decide whether to decline or overlook the payment (Domashova & Zabelina, 2021).

The tasks that anti-fraud systems are designed to solve include the following (Liao & Yang, 2018):

- minimization of the level of fraud;
- maintaining a high level of customer loyalty through correctly identified fraudulent transactions, as well as through the successful processing of legitimate transactions;
- ensuring information exchange with the regulator established by law.

The antifraud system consists of several components (Eni-Olorunda et al., 2020):

- automated transaction surveillance that entails numerous customizable filters;

- procedures for verifying the authenticity of the cardholder and validating the card;
- monitoring of transactions in the "manual" mode for extreme cases.

The system can include hundreds of different filters, and the more the business area is prone to fraudulent activities, the more filters are included and the more detailed each of them is configured for a specific online store or online service (Prasad & Venugopal, 2020). Fraud monitoring systems do not work perfectly, therefore, in order to avoid possible unpleasant situations, it is necessary to check orders manually. Automated transaction surveillance that entails numerous customizable filters.

This part of the thesis describes both the functional and non-functional competences of the major anti-fraud tools. However, to perform a proper review and relative analysis, it's crucial to list some standards according to which we can assess different anti-fraud software. The functional requirements, an up-to-date anti-fraud software has to possess, include requirements for integration and iteration, requirements for online module operation, requirements for the investigation module. As for such requirements' characteristics, they are the following:

Characteristics of requirements for integration and interaction (Nweke & Asogwa, 2020):

- Transactions from multiple cross-channel sources should be observed and validated. This can prevent fraudulent activity from migrating between channels. Examples include card processing and RBS.
- There should be the ability to integrate with different data sources of the customer to gain information about their non-financial activities. Examples include CRM information about the client's agreements or about their cards' issuance.

Characteristics of requirements for online module operation (Prasad & Venugopal, 2020):

- The rules of the interface should possess rapid, adaptable settings to conclude if fraudhas taken place. For instance, the rules for the process of identifying fraudulent activity are specific to each bank, region, channel, etc. Anti-fraud rules should consider a bank's expertise and analyze historical data in each case. Indeed, fraudsters adapt fast and then modify of even change their tactics. Therefore, anti-fraud systems should allow for equally fast rule modifications.
- There should be the ability to incorporate machine learning methods during monitoring.
- There should be the ability to access information from data warehouses when proving transactions, making downloading and updating data in the online module more convenient.
- There should be the ability to test different scenarios based on historical data.

Characteristics of requirements for the investigation module (Mwema & Mamboleo, 2018):

- There should be the ability to conveniently integrate the online module with the investigation module to spread information about doubtful operations. Integration should be direct and not involve additional technical processes.
- There should be the ability to present interface information from the data warehouse that is vital for carrying out the investigation. Such information can be about the client, their operations, their cards and agreements, etc.
- There should be the ability to download the updated information that can be instantly displayed via the interface. During examinations, bank employees (who work at the anti-fraud department) require access to the most significant client information. Consequently, the information system should regularly update that information.

The characteristics of non-functional requirements anti-fraud tools have to encounter are the following (Chen & Chen, 2020):

- When the online module has a high grade of fault tolerance, it implies continuous operation. This raises the possibility of using a backup productive circuit in case of an emergency on the active one.
- Vendor technical assistance should be available.
- Users should be able to modify and customize the software deprived of involving a vendor.
- A documented API should be possessed.

It's challenging to perform a comparative study when not having any practice in using such tools. Indeed, most vendor websites simply list opportunities and benefits. This makes finding a given system's limitations more challenging. As a rule, solutions from big vendors retain similar functionality. In the research done by Davenport & Milburn (2021) it is suggested to observe non-functional characteristics as the ones to make the core differences. They include (Davenport & Milburn, 2021):

- license cost;
- scalability;
- quick system setup convenience;
- technical support quality.

The variety of tools provided here stem from a market evaluation prepared by the 360quadrants agency (2021). The research done presents the following solutions:

- IBM Safer Payments;
- FICO Falcon Platform;
- SAS Fraud and Security Intelligence;
- NetReveal BAE System.

1.6.1 IBM Safer Payments

This is an overall platform for analytics based on the Integrated Rule Inference System (IRIS) platform. It is aimed at spotting fraud attempts at present. It simultaneously ensures security when users make non-cash payments in different systems (such as automated clearing houses, acquiring banks, the Single Euro Payments Area, Chip and Pins, etc.) and via POS terminals, ATMs, and online or mobile banks. Product Features:

- the tools utilizes machine learning technology to stop fraud and the approaches used are adaptable enough to export models in Predictive Model Markup Language (PMML) format;
- the rule development interface requires no coding knowledge;
- investigation interfaces are not customizable;
- preconfigured policies allow customer alteration without vendor participation;
- the input system admits merely a flat data vector without nested structures;
- it offers various integration protocols that enable the file uploads, the database integration to be carried out online, etc.;
- it features both online and offline components and is not distributed in a modular manner.

1.6.2 FICO Falcon Platform

This software enables the compliance with regulatory requirements such as a *system of technical support for combating the spread of information related to security* (It is designed to ensure compliance with regulatory requirements related to information security in Russia. The measures within it consist of actions aimed at stopping the unauthorized release of private data, like personal information, and protect from cybersecurity breaches and other types of security risks. The specific requirements and guidelines for compliance with this system are determined by the Russian government and may vary depending on the industry and sector.) by identifying attempts of stealing identities and any other ways of combating fraudulent activities in Internet banking or other online services. The platform also watches system administrator and privileged user activity while tracking the accessibility and reaction time of serious processes. Also, it monitors all occurrences of given or taken PIN codes. Lastly, it tracks any multi-location transactions made on the same account in a short period of time.

1.6.3 SAS Fraud and Security Intelligence

This suite of the general product contains anti-fraud tool for banking, the public sector, healthcare, insurance, anti-fraud, and money laundering. Moreover, there is the SAS Fraud Management application (being a part of the whole SAS Fraud and Security Intelligence product). It is a cross-channel anti-fraud product for preventing transactional frauds and is intended for execution in the banking sector.

SAS FM features an already built data model for the integration module. This includes a great list of attributes separated in some blocks such as general information, client, account, device, authorization, etc.

As is stated by the vendor, it's required to link together the message from an external system and the SAS FM data model so to realize incorporations with other systems. It is set that the process of sending messages to the system's internal database is formed. Therefore, new integrations rely on the both integration module and mapping technical formation.

SAS FM also enables rules' development. It includes some function modes, which are drag-and-drop and coding. Users are able to use historical data to test the rules, while the system sets the minimum criteria lists for the rule to operate.

SAS FM can create warnings once specific circumstances are trigged and furtherly perform immediate analyses. However, this model of investigating is not customizable and shows limited functionality. Consequently, even though there is an effective integral incident-management module, the vendor recommends applying SAS FM alongside the SAS Visual Investigator. The latter platform has an adaptable and customizable user interface and can carry out investigations in one banking system, not requiring additional data from others. For instance, through an investigation, an anti-fraud employee can be provided with client' information, their transactional activity, their cards, and other banking products.

1.6.4 NetReveal BAE Systems

The NetReveal British Aerospace Engineering (BAE) software was designed to help financial institutions stop Internet fraud. It accomplishes this objective by monitoring the actions users take, including logins, failed logins, profile changes, and cashless money transfers through an online monitoring module called Risk Engine.

The tool includes an inventory of lots of different indicators that facilitate the detection of fraud. Some of the indicators include the transaction volume, IP address, latest account opening, and more. Each of the actions is provided a "risk score" built on the rate of the indicators, which makes fraud detection possible.

The algorithm of identifying an attack profile combines several parameters and uses that data to evaluate the "risk score" by means of the Bayesian network principle. Then, a special statistical model is operated to assess risk. This is done by considering all the signs and calculating the probability of fraud (or risk of it) associated with the activity that's being analyzed. It is not only able to identify patterns of an attack, but it is also able to leverage the outcomes of examinations conducted by the Anti-Fraud Command Center.

The NetReveal BAE tool also offers a Case Management module that analyzes suspicious operations. All the actions that receive a score of a high-risk by the Risk Engine module are

recorded in the Investigations module. The results of those investigations are then included in the Online module automatically. This module offers many different functions for systems such as observing warnings and their automatic ranking, as well as creating an assessment for each incident. The tool leverages clustering and coloring proprietary processes. The clustering simply combines the transactions with several characteristics in common, such as IP address, type of device, user, etc. While a transaction is being examined, the clusters to that the operation belongs to are taken into account for the analysis as well. When a transaction is classified as a fraudulent one, the coloring process will color the whole cluster to indicate that every transaction in that cluster has a higher level of risk.

Additionally, the NetReveal BAE offers a Policy Manager module that allows the bank to use its risk management policy. That means that the module adopts a set of custom rules, which can be tested and adapted as necessary in the development interface that the system provides.

When it comes to interaction of integration, the NetReveal BAE can assume these potential varieties: Web Services Simple Object Access Protocol (SOAP) API, Log File Analysis, and HTML Beacon (An HTML Beacon is a code snippet that's inserted into a web page or email, allowing a third-party server to gather information about user behavior. These beacons are usually invisible to users and can track various activities, including email opens, link clicks, page views, clicks, and form submissions. They are commonly used in email marketing campaigns and web analytics to measure user engagement and track user behavior). The Log File Analysis wouldn’t require integration with the banking system because it uses the data stored in log files, so users can start the system right away before executing the API.

1.6.5 Comparison

The information used to describe the existing solutions, that have been previously laid out, has been gathered using the method of literature review, in particular 360quadrants agency review, and several articles about these antifraud tools. Moreover, Mr. Andrey Pilipchuk (a bank X representative who has been interviewed for this master thesis) has shared his and his team’s thoughts about the existing solutions. Based on the above mentioned collected information, the author of this master thesis suggests the following comparison of the existing solutions:

- ease of integration implementation;
- accessibility and functionality of online monitoring processes and of the module for investigating;
- non-functional features such as system customization options, license cost, support quality, and more.

The description of how each tool reflects to all of the four comparison items has been done by studying and analyzing information obtained from the 360quadrants agency, articles, and the interview. The Table 5 offers a summary.

Table 5: Comparative descriptions of different anti-fraud software

	Integration/cross-channel	**Online module**	**Case Management**	**Non-functional characteristics**
IBM Safer Payments	Processes only "flat events", which means that there is no possibility to receive events with nested structures.	High quality of realization of operations' online verification step. The interface for setting up rules is not customizable, there is no way to write custom code.	It is not possible to configure the output of information in the interface, as well as not possible to set the work with warnings.	Technical support from the vendor is available in several counties, but not in Russian Federation.
FICO Falcon Platform	The system only checks transactions on the Internet. A separate system is required to verify card transactions.	High quality of implementation of operations' online verification. There are also technologies implemented that can enable teaching validation rules based on information coming into the system from different sources.	It is not possible to configure the output of information in the interface, as well as not possible to set the work with warnings.	Technical support from the vendor is available in several counties, but not in Russian Federation.

To be continued

Table 5: Comparative descriptions of different anti-fraud software *(cont.)*

SAS Fraud and Security Intelligence	The system implements a data model for incoming events. Adding new attributes by regular means is not provided.	It is possible to set up rules for checking operations, using data on the client's historical activity. There is no need for customization to add a new historical indicator.	The SAS Fraud Management system implements a non-customizable module for conducting investigations. When implementing SFM together with SAS Visual Investigator, it is possible to flexibly configure interfaces and work with warnings.	Availability of Russian and global technical support. In the work of SAS VI, systemic problems were identified in the operation of the mechanism for updating transactional data in interfaces.
NetReveal	There is analysis of information about customer activity in Internet channels. To analyze card transactions, a third-party IS is needed, so there is no cross-channel.	There is a module with a large number of configured risk indicators, as well as there is the ability to configure verification rules based on the bank's expertise.	It is not possible to configure the output of information in the interface, as well not possible to set the work with warnings.	Technical support from the vendor is available in several counties, but not in Russian Federation; high cost of licenses.

Source: own work.

According to several studies (Osei-Assibey & Kwarteng, 2020; Ashbaugh-Skaife & Sanchez, 2020), the quality of an anti-fraud system can be enhanced when the following factors happen:

– scenario of confirming an operation match the current fraud patterns and rapidly adjust to the changes in schemes practiced by fraudsters;
– through verifying the transaction, client’s historical information is consumed, labeling

typical for the client's transactional and non-financial activity;
- regarding verifying the transaction, data from different channels is taken into account, enabling the information about the behavior of the client at its fullest;
- high fault tolerance of the system guarantees constant processing of incoming events.

The first point can be reached if the workers of the bank's anti-fraud department possess a high level of proficiency; and also, when modifications to the logic of proving transactions in the anti-fraud system can be introduced quickly. The second point (which uses the historical data about the client's activity) can greatly impact the quality of the anti-fraud system. It is also dependent on the level of bank employees' proficiency or on the level of crucial expertise of the consultants who put into service the fraud-combating information system. The other points can be executed with the help of special functionality of the particular information system applied in the bank.

This part of the thesis outlines the execution of the anti-fraud process in financial institutions. Four anti-fraud areas (requiring balanced development) that demand work have been pointed out:

- preventing transaction fraud;
- preventing internal fraud;
- cooperating with the regulator concerning information exchange on transactions made without clients' approval;
- information security.

Implementing anti-fraud processes in financial institutions is unmanageable without the consumption of IS. Requirements for up-to-date anti-fraud systems has been compiled, as well as evaluation criteria has been created. These was done using data about stolen funds and information about different fraud approaches.

One of the most vital requirements seems to be the capability to rapidly adapt the system to respond to fraudsters' ever-evolving actions. To be able to perform this, the system must provide a development interface that is convenient for users. This section of the thesis overviews and compares the major anti-fraud systems available on the global market.

It is worth stating that great supplies and effort are needed for implementing and maintaining an information system, as the desired system has to be effective at fraud fighting. To implement an information system, there has to be an analysis of the banking processes to detect the areas that are most vulnerable to the actions of fraudsters.

Then, the bank has to put together employees that will focus exclusively on the anti-fraud system. Even if the bank uses a consulting firm to implement the anti-fraud system, it is still essential to have a competent team that can handle the system's operation. The members of the team have to be administrators (to administer the system), analysts (to observe the applicability of the anti-fraud system rationality), and others (to perform supplementary

evaluations of suspicious operations). Delegating all the work to contractors can eventually lead to an unmanageable system. Should that happen, the system will not be able to accomplish its intentions and purposes.

Following the outline given in this section, the following points were presented:

- study of national and international characteristics of financial institution activities within the context of the process of managing risks and legal framework in this subject;
- statistical data examination of the stolen funds and significant modern fraud approaches;
- exploration of a usual process of countering fraud in financial institutions based on the information and analytical systems;
- comparative analysis of the common anti-fraud systems with a focus on their functionality and the technical sides of operation.

2 DESCRIPTION OF THE CURRENT ANTI-FRAUD PROCESS IN THE LARGE RUSSIAN BANK

The purpose of this chapter is to describe and analyze the current anti-fraud process in a large Russian bank, including research on the bank's activity and a description and analysis of the as-is anti-fraud process. The main parts of this chapter include a research on the Bank X’s activity and a description and analysis of the as-is anti-fraud process in the bank.

These parts provide a detailed overview of the anti-fraud process currently in place in the bank, including any strengths and weaknesses, as well as any opportunities for improvement. This section performs a basis of the subsequent chapter on improving the fraud detecting process.

A mix of primary and secondary research methods is utilized to acquire information for the study. The primary research involved conducting an interview with a representative from Bank X to gain firsthand knowledge of their anti-fraud process. This method of data collection is known as qualitative research and can provide valuable insights into specific processes, practices, and experiences. The secondary research involved conducting a literature review by reading academic articles, news articles, and industry reports to gain a broader understanding of the current state of the banking industry and its anti-fraud processes. This method of data collection is known as quantitative research and can provide a more comprehensive view of a particular topic or issue.

By combining both primary and secondary research methods, it was possible to gather a variety of information to be used in this study. The primary research provided the specific details and insights into Bank X's anti-fraud process, while the secondary research provided a broader understanding of the banking industry and current anti-fraud trends and practices.

In addition to the primary and secondary research methods described earlier, the methodology also involved using data from open sources about the bank X activity. The use of open sources included collecting data and information from publicly available sources, such as news articles, the bank's website, and regulatory reports.

2.1 Research on the Bank X's activity

Bank X is a Russian retail bank founded in 2016 as a joint venture between a giant banking group and a Russian Post group. Banking services are offered to over 15 million customers using the Russian postal network and banking branches. These service points exist as customer centers (branch offices), sales counters, and POS units in stores. By the end of 2018, the bank had 50,000 POS units across 37,000 branches, and the first nine months of 2021 saw the bank opening over 19,000 service points in 83 regions of the Russian Federation, of which more than 80% were in small settlements and rural regions.

The bank's customer service agents are post office staff specially educated to operate the POS terminals and receive money bonuses for fulfilling transactions. Products and services include providing loans (including education ones), issuing credit and debit cards, accepting deposits, arranging pension transfers, payroll projects, and small business assistances.

Bank X has expressed a commitment to enhancing the customer service experience through consistent technological innovation and diverse service integrations. For instance, in July 2019, the bank implemented a system to confirm various transaction types (such as deposits closing, transfers, and payments) using selfies—a first in Russia. The facial recognition solution uses the data about the client's behavior and biometric photo identification and is created using the VisionLabs Luna platform used in RBS and relies on image processing and analysis.

Beyond this, Bank X was also the first Russian financial institution to enrich its mobile and internet banking services with Real-Time Marketing technology—a CRM innovation applicable to remote customer service channels. The artificial intelligence-driven system enables immediate and real-time personalized offer based on the client's data and the nature of the application submitted.

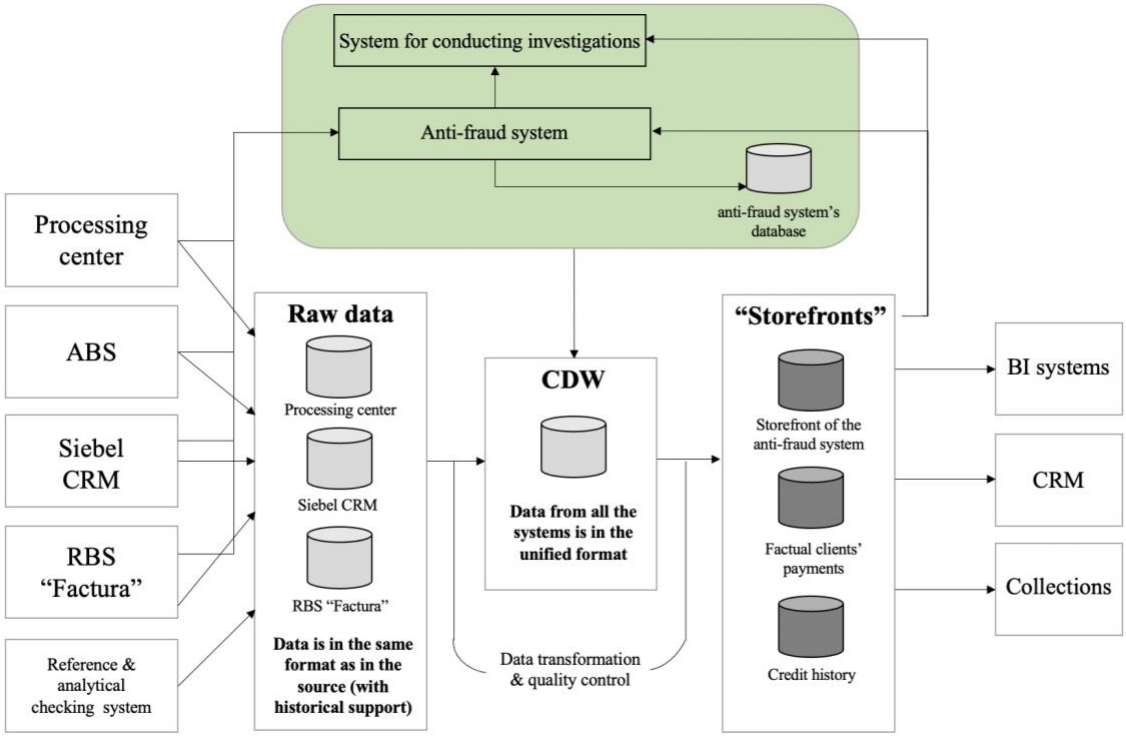
At the end of July 2020, the bank had the largest POS loan portfolio in Russia. Based on data from Frank RG, its commodity loan portfolio totaled RUB 42.8 billion, showing an increase of 1.1 billion over the month. Additionally, the accredited capital of the bank is 860 million of rubles. Net profit amounted to RUB 6.4 billion over the past year, a decrease of 0.4 billion compared to the previous year.

In the 12 months of 2021, the bank's net interest income grew by 11% to RUB 44.5 billion. Net fee and commission income enlarged by 4% to RUB 32.3 billion, and operating expenses totaled RUB 38.8 billion, a reduction of 1.5 billion (4%) in comparison with 2019. Assets

increased to RUB 474 billion from RUB 472 billion at the beginning of 2020. The bank's loan portfolio also boosted by 9% to RUB 450 billion. And finally, the cash loan portfolio raised by 10% to RUB 379 billion from RUB 344 billion at the beginning of the year.

Bank X's anti-fraud process can be understood by first analyzing the high-level architecture of the bank's information systems (Figure 6). The scheme was first explained by bank X representative Mr. Pilipchuk to the author of the thesis. Based on this discussion and several according articles, the outline of information systems was created, which was then shown to the representative for approval. While this scheme does not aim to comprehensively describe all its architectural modules (being aggregative), it sufficiently captures those aspects relevant to the agenda of this thesis.

Figure 7: The high-level architecture of the bank X's information systems



Source: own work based on Andrey Pilipchuk (personal communication, November 2022).

Separate application databases are used to store historical data from the systems used by the bank. Upon collection, this information undergoes a number of transformations to standardize its structure and keys. During this process, the data is cleaned and checked for quality, while data consistency and integrity are ensured. Consequently, a corporate data warehouse (CDW) is created. This unified and standardized CDW data enables the development of various storefront consumer systems based on specific bank departments' business requests, such as BI or CRM systems, anti-fraud systems, and systems that monitor overdue debts for the Collection division.

The bank’s architectural features relevant to the aims of this work are highlighted with green on the figure. Data required for the anti-fraud process enters the anti-fraud system to be verified and analyzed. Data about the system’s operation is stored in the anti-fraud system’s database and then undergoes the transformation procedure for being stored in CDW. Research on the Bank X’s anti-fraud process is shown in the following part.

2.2 Description and analysis of the as-is anti-fraud process in the bank

This part represents the comprehensive analysis of the Bank X’s anti-fraud process. The used methodology for the research has been focused on gathering information about Bank X's anti-fraud process, with a specific focus on the information system used by the bank. During the interview, topic-related questions were discussed in order to gain understanding of Bank X's anti-fraud process, including ones about technology systems and tools used by the bank. The representative from Bank X provided detailed information about their anti-fraud system and how it is used within the bank's anti-fraud process. Based on the information obtained during the interview, additional research and analysis were conducted to further understand the anti-fraud system and how it works within the bank's anti-fraud process, reviewing available documentation in particular.

The bank uses the Russian development "Antifraud.Internet" as an anti-fraud system to combat fraud in Internet banking. "Antifraud.Internet" is the solution developed by the Russian IT company which is designed to combat fraud in Internet banking. It allows the bank to monitor customer transactions through Internet banking and detect potentially fraudulent activities.

The service is made up of multiple applications that are hosted on Microsoft Azure. It is consisting of several systems:

1. the Antifraud.Internet API Service which is a Representational State Transfer service that offers an API for communication with the Fraud Predictor ML.
2. the Antifraud.Internet Fraud Predictor ML which is responsible for detecting fraudulent payments using machine learning tecniques;
3. the Antifraud.Internet Transactions Log which is a NoSQL storage for transaction information.

To be more precise, this anti-fraud model uses machine learning algorithms (such as decision trees, logistic regression, and neural networks) to detect fraudulent transactions based on data from previous transactions. This model consists of several components, including a transaction log, an API request processing service, and machine learning algorithms to detect fraudulent transactions. The first block collects data about the client and his transactions, providing an interface for interacting with the model. The data then passes through a pre-processor where it is cleaned of noise and anomalies. Next, the data is sent to the transaction log, where it is converted into numerical values that can be used in machine learning

algorithms. This allows to find patterns that are characteristic of fraudulent transactions. The transaction log contains information about previous transactions, such as time, amount, location, and other details. This data is used to build and train a machine learning model. Afterwards, the data undergoes a classification process which decides whether the operation is fraudulent. In case the transaction is identified as fraudulent, it is stopped and forwarded for further investigation.

Machine learning algorithms are used to identify fraudulent transactions based on learning from previous transactions. The algorithms use methods such as decision trees and random forest to classify transactions as fraudulent or legitimate. If a transaction is classified as fraudulent, then it is marked as suspicious and can be checked for additional details.

Overall, this model uses data from previous transactions and machine learning algorithms to automatically detect fraudulent transactions and protect against financial losses associated with fraud.

This system's work characteristics are the following:

- transaction monitoring: the system monitors all transactions carried out in Internet banking and analyzes them for signs of fraud; during the analysis, the system uses various machine learning algorithms and statistical methods;
- risk assessment: the system determines the risks for each transaction based on a number of factors, such as the amount of the transaction, the place and time of the transaction, the client's transaction history, and other parameters;
- blocking fraudulent transactions: if the system detects signs of fraud, it can block the transaction and send an alert about possible fraudulent activity to the bank staff or the client;
- data analysis: the system collects data on fraudulent transactions and analyzes them to identify patterns and form profiles of fraudsters; this helps improve system efficiency and prevent repeat fraud.

The representative also shared some rules that their anti-fraud system uses (not all the rules because this data must not be publicly available); these are geographical rules. There is a list of allowed countries (Russia and CIS countries). Accordingly, top-up transactions are only allowed from IP addresses in these countries, and all others are prohibited. Another rule checks for a match between the user's IP location and the issuer country. A common geographical area has been created for Russia and the CIS countries to top up an account from Ukraine with a Russian card.

However, based on the information obtained from the interview, the system has several disadvantages. For example, as it was found out that it is an often-repeating case when the bank's fraud detection system flags legitimate transactions as fraudulent and blocks them, causing inconvenience and frustration to the customer. In the opinion of bank's

representative, this happens because "Antifraud.Internet" is overly aggressive and relies too heavily on automated rules and algorithms without considering the nuances of individual transactions. For example, a customer may be traveling to a foreign country and using their credit card to make purchases, which can trigger a fraud alert because the bank's system does not recognize the unusual spending pattern. Sometimes the bank blocks the transaction without first verifying with the customer, which leads to a negative experience and can potentially cause the customer to switch to a different bank.

Another example of bad anti-fraud management that bank X's anti-fraud office often faces is when "Antifraud.Internet" fails to detect actual fraud and allows fraudulent transactions to go through. This can happen if the system is not properly calibrated or if fraudsters find ways to bypass the system's controls. In such cases, the bank suffers financial losses and damage to its reputation, as well as loses the trust of its customers. Additionally, the representative points out the case when this system is not able to respond to cases where a person who has never taken out a loan before suddenly takes out a loan for hundreds of thousands and immediately transfers the funds to another individual's card.

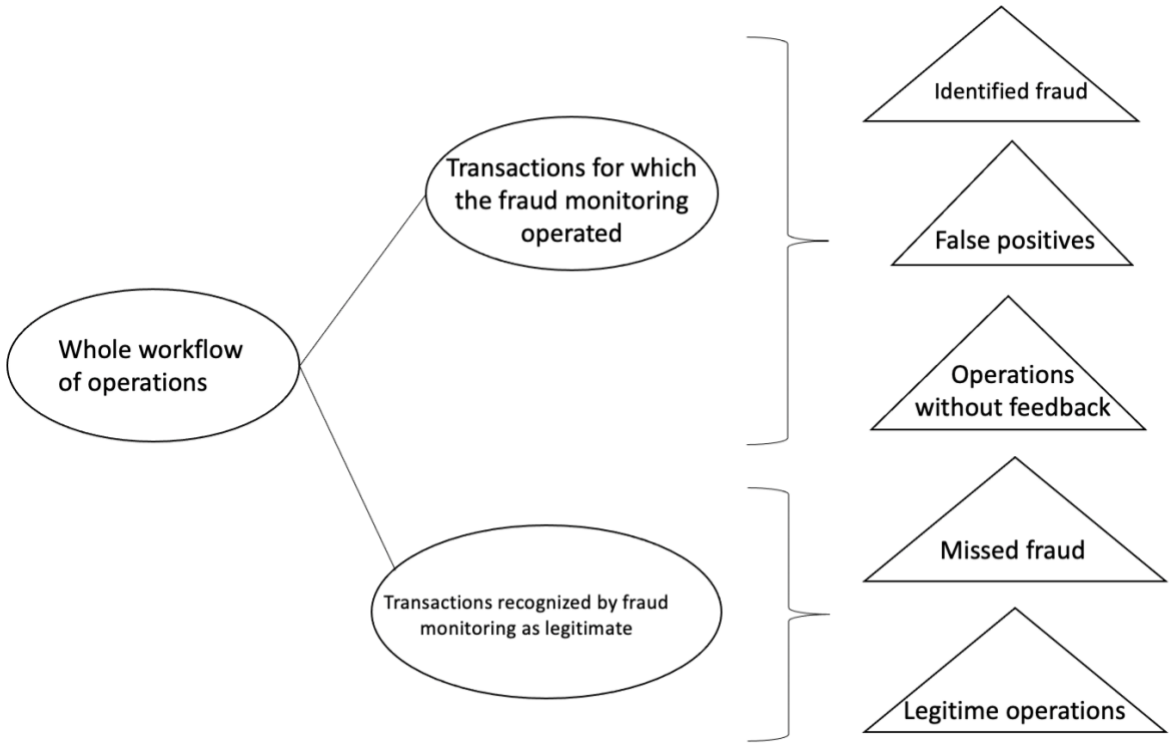
Together with a representative of the bank, we identified the shortcomings of the Antifraud.Internet system:

- technical limitations that affect the performance of machine learning models: the need for large volumes of data and computational resources, resulting in longer processing times, increased costs, and scalability issues;
- fraudsters may try to manipulate the system through adversarial attacks, such as generating fake data or reverse engineering the system to find weaknesses and avoid detection;
- inability to handle new types of fraud: the system may not be effective in combating new types of fraud that were not taken into account when it was created;
- false positives: the system may block some legitimate customer transactions, which may cause dissatisfaction and loss of confidence in the bank;
- inefficiency: the system may not process transactions fast enough or use too many resources, which can negatively impact the customer experience;
- difficulties with implementation: the system may require significant investments from the bank and difficulties with its implementation and configuration;
- low accuracy of fraud detection: the system may not always detect fraudulent transactions, which can lead to financial losses for the bank;
- data quality: it is crucial for machine learning models, as their accuracy and effectiveness depend on the quality of the data used for training; if the data is not representative, biased, or incomplete, it can negatively affect the performance of the system.

Criteria for Determining the Quality of Anti-fraud Systems

To determine the effectiveness of an anti-fraud system, criteria introduction is needed. To define the approach for identifying such criteria, it is crucial to identify all potential consequences of verification procedures. These are indicated in Figure 7. Transactions for which anti-fraud measures were successful contain both fraudulent and legitimate transactions and those that received no feedback from clients. At the same time, transactions for which an anti-fraud system were not successful contain legitimate and fraudulent transactions.

Figure 8: Possible outcomes of checking operations in the anti-fraud system



Source: own work.

In order to enhance quality of an anti-fraud system, the following measures should be taken (Islam et al., 2020):

- decrease the number of false positives;
- decrease the number of missed fraudulent transactions;
- rise the number of identified fraudulent transactions;
- decrease the part of transactions when system proved effective but in which anti-fraud officers did not succeed in reaching the client and gaining data regarding the legitimacy of such transactions.

In order to evaluate how successfully the antifraud system works, it is proposed to initiated this system of measurement:

Missed Fraud (MF) = number of transactions recognized by fraud monitoring as legitime / the number of operations that enter the anti-fraud system.

False-Positive Fraud (FPF) = number of legitimate transactions that were recognized as fraudulent by the anti-fraud system / (number of legitimate transactions that were recognized as fraudulent by the anti-fraud system + the number of identified frauds + number of operations for which the system worked, but the anti-fraud officers failed to contact the client and obtain information about the legitimacy of the operation)

One of the key aims of an anti-fraud process lies in decreasing the MF and FPF. As of the position of the anti-fraud process, errors concerning the FPF are more serious: stolen client money is mostly unmanageable to get back. Errors concerning MF are not that dangerous, however, they have a destructive effect on the bank client loyalty. Customer assurance about the bank can be lowered if there too many forbidden or suspended legitimate transactions happen. Also, it should be pointed out that calculations of the FPF value considers the amount of operations that the anti-fraud system identified as fraudulent ones, but for which the client could not be reached out to authorize the system's accuracy. The more those transactions occur, the lower the FPF is. Earlier, it was stated that one of the issues of verifying client transactions is the effort of keeping an up-to-date database of bank customers contacts. Also, little customer assurance in calls from the bank takes place, as fraudsters frequently contact customers by phone and identify themselves as bank employees. Consequently, when calculating the FPF, it is essential to study the number of false positives and the number of transactions when clients failed to be reached out individually.

The quality of an anti-fraud system can be enhanced when the following factors happen (Mustafa & Ghazali, 2021):

- scenario of confirming an operation match the current fraud patterns and rapidly adjust to the changes in schemes practiced by fraudsters;
- through verifying the transaction, client's historical information is consumed, labeling typical for the client's transactional and non-financial activity;
- regarding verifying the transaction, data from different channels is taken into account, enabling the information about the behavior of the client at its fullest;
- high fault tolerance of the system guarantees constant processing of incoming events.

The first point can be reached if the workers of the bank's anti-fraud department possess a high level of proficiency; and also, when modifications to the logic of proving transactions in the anti-fraud system can be introduced quickly. The second point (which uses the historical data about the client's activity) can greatly impact the quality of the anti-fraud system. It is also dependent on the level of bank employees' proficiency or on the level of

crucial expertise of the consultants who put into service the fraud-combating information system. The other points can be executed with the help of special functionality of the particular information system applied in the bank.

Current state of the process

In an anti-fraud system, it is crucial for customer to have a possibility of online transactions verification. There are several points rooting for the high accuracy of online detection of fraudulent transactions:

- high-quality online verification assists to decrease the burden on anti-fraud officers, because less operations will be postponed pending investigation;
- if there are many false positives generated by anti-fraud procedures that result from a low quality of online verification, a decrease in customer loyalty due to frequent suspension of operations can occur;
- lessening the human factor influence when forming a decision on a suspicious transaction, as such decisions are made with the help of online verification.

The rules for verifying transactions in the system are invented in compliance with the bank's capability. The data used to authorize a transaction is:

- attributes of the current operation;
- data on the client's operations and the non-financial activity during several days before the transaction happened;
- some “black” lists of clients or devices;
- catalogs of risky terminals or countries;
- data about the client himself and about their banking products.

To analyze the quality of an anti-fraud system, it is essential to calculate the values of MF (which characterizes the proportion of missed fraudulent operations) and FPF (which illustrates the ratio of false positives identified by the system).

The approach for determining these indicators is to make SQL queries to reach the anti-fraud system database. That was suggested to do to the Bank X representative who has access to the databases. The columns that are being used contain the following data:

- all customer operations;
- non-financial operations of the client (for example, logging into the application or renewing the password);
- operations that were acknowledged as fraudulent ones;
- alerts generated by the anti-fraud system;
- information about the status of alerts.

The bank X's representative shared the data that represents the figures for MF and FPF that were calculated with access to their databases. The time period for which the indicators are calculated is carried out is the first quarter of year 2021. Due to the fact that the data is confidential, only the results of calculation can be shown (however, the formulas used were the ones that were suggested by the author):

- Missed Fraud (MF) = number of transactions recognized by fraud monitoring as legitime / the number of operations that enter the anti-fraud system; MF = 0,000183;
- False-Positive Fraud (FPF) = number of legitimate transactions that were recognized as fraudulent by the anti-fraud system / (number of legitimate transactions that were recognized as fraudulent by the anti-fraud system + the number of identified frauds + number of operations for which the system worked, but the anti-fraud officers failed to contact the client and obtain information about the legitimacy of the operation); FPF = 0,72.

Together with the bank representative it was decided that the anti-fraud system has to be able to work so effectively that the standards of missed fraud (MF) should be 0,00015 and false-positive fraud (FPF) should be 0,5. This means that at the moment results of the current anti-fraud system's work do not match the goal. The MF values differs from the target by 18% (1 – 0,00015/0,000183), and the FPF ones by 30% (1 – 0,5/0,72).

3 IMPROVING THE CURRENT FRAUD DETECTING PROCESS

Through the research, it has been identified that the bank's current antifraud system is facing several limitations, such as low accuracy of fraud detection, false positives, and inefficient processing of transactions. To overcome these challenges, it was suggested to introduce SAS Fraud and Security Intelligence system (which includes the SAS Antifraud package) as the bank's antifraud system.

In this study, the following factors have been considered based on the information gained through various sources: the accuracy of the system in detecting fraudulent transactions, the system's ability to handle large volumes of data, the level of customization and flexibility offered by the system, and the ease of implementation and use.

Based on the author's evaluation, it has been concluded that the SAS Antifraud system is the most suitable option for the bank. The system's specific features such as advanced machine learning algorithms, real-time detection capabilities, and the ability to detect new and emerging types of fraud make it a good fit. Additionally, you may have highlighted the success stories of other financial institutions that have implemented the SAS Antifraud system.

Overall, the decision to recommend SAS Antifraud as the bank's antifraud system has been based on careful research, evaluation of available options, and consideration of the unique needs and requirements of the bank.

Based on an interview conducted to explore ways of improving the current anti-fraud process, the bank representative mentioned the possibility of completely changing the vendor. This suggestion gave the author of the thesis an idea of implementing SAS Antifraud system as the bank's antifraud system. This proposal was discussed with a representative from the bank, and there had been a detailed conversation about the capabilities of SAS Antifraud and how it could be integrated into the bank's existing infrastructure. The representative acknowledged the limitations of the current system and agreed that implementing SAS Antifraud could be helpful in optimizing the fraud detecting process, however there must be qualified research done beforehand.

3.1 SAS Antifraud description

The workflow of SAS Antifraud can be described as following (Zhang & Yuan, 2020):

- Data Collection: the system collects customer transaction data as well as other data such as customer and risk information;
- Data Analysis: the system analyzes data using various machine learning algorithms and statistical methods to identify anomalies that may indicate fraudulent activity;
- Risk Assessment: the system evaluates the risks of each transaction based on various factors such as the amount of the transaction, the location and time of the transaction, the client's transaction history, and other parameters;
- Fraud Detection: the system determines if a transaction has signs of fraud and takes appropriate action to block or delay it.
- Learning: the system constantly learns from new data and improves with various machine learning algorithms to detect all new types of fraud.

So, summing up, SAS Anti-Fraud is highly flexible and can be configured to deal with different types of fraud and different types of financial institutions. It is also applicable for the identification of fraudulent practices in other fields, including retail and insurance.

3.1.1 SAS Antifraud process flow

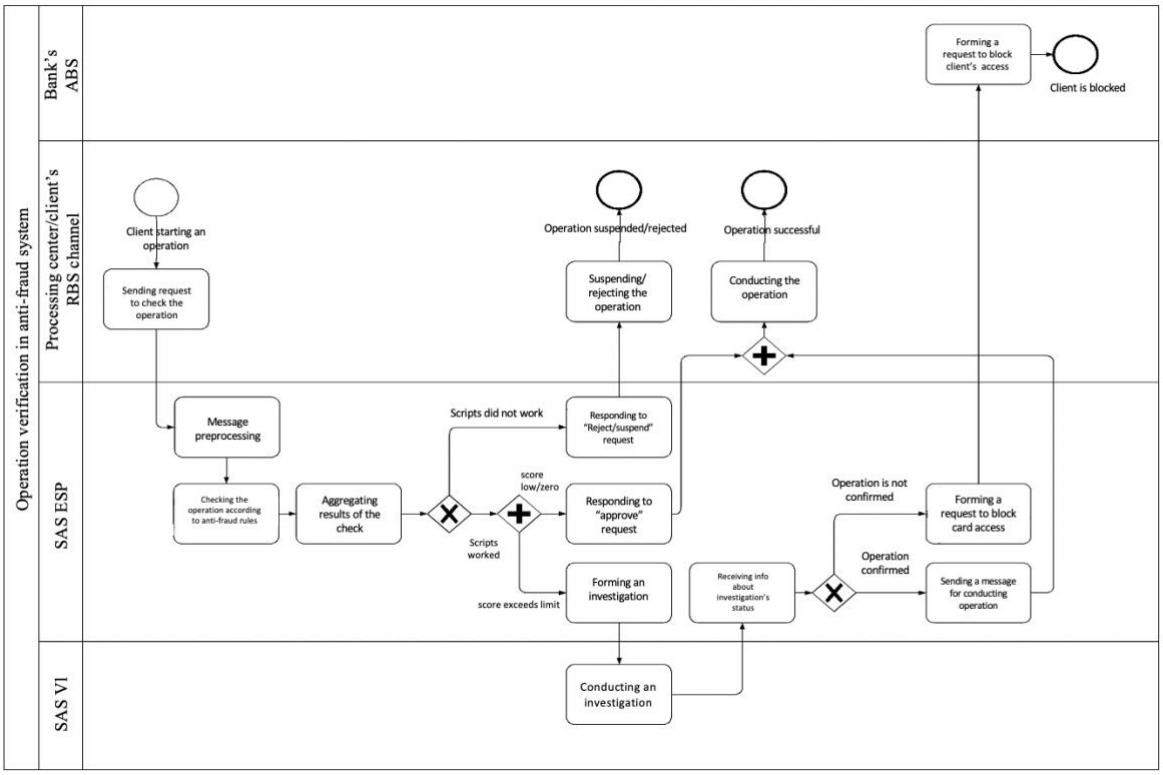
The description of the process with the SAS Antifraud can be the following: first, the client starts a card operation at a POS terminal, ATM, or alternative channel. Next, the transaction is registered and transmitted to the anti-fraud system’s online module, which evaluates it based on several anti-fraud setups. The verification process also manages specially arranged rules that, beyond checking the operation data itself, check recent customer activity during a few days and compare the nature of the current transaction to the typical transaction the

client makes. Using the result of this verification, the processing center is directed to either carry on, suspend, or reject the transaction. Simultaneously, a warning is sent to the system, and an anti-fraud officer carries out an investigation to either confirm the operation or mark it as fraudulent. If the investigation concludes that the operation is fraudulent, a warning is sent to the automated banking system (ABS) to block the card forever or revoke its access to the remote banking service. If the operation is deemed authentic, a message is sent to execute the operation.

3.1.2 Operation verification scheme in SAS Antifraud process flow

In this study, a scheme to verify anti-fraud operations was developed. To do this, information from different open-source resources was gathered, and also the author sought assistance from a representative of Bank X who is a professional in anti-fraud operations. This representative was able to provide insights into how such systems are constructed, which helped to develop this verification scheme for this study, as depicted in Figure 8. He also contributed to the part of explaining information flows by checking and approving it after making small corrections in the flows and their distributions. His opinion counted given the possessed experience.

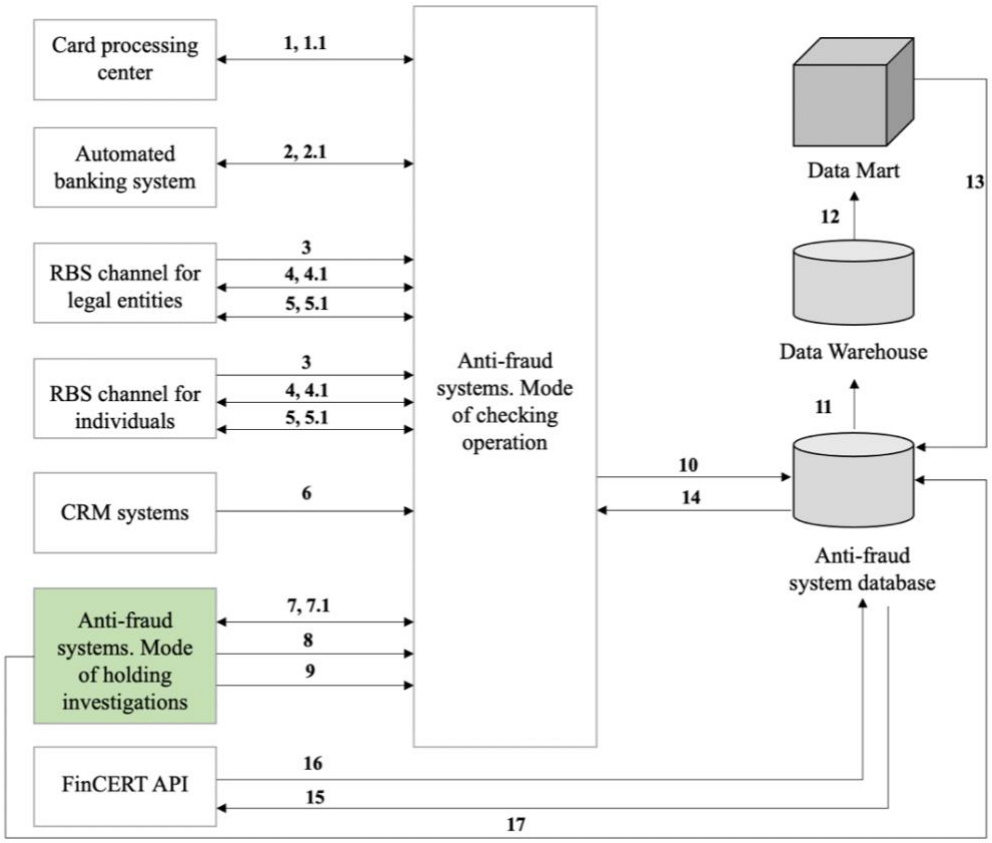
Figure 9: Scheme of the process of combating fraud using information systems



Source: own work based on Andrey Pilipchuk (personal communication, February 2023).

An information flow diagram based on these processes is shown in Figure 9, which describes the anti-fraud system's components and the external systems integrated with its online module.

Figure 10: Scheme of information flows of the anti-fraud system



Source: own work based on Andrey Pilipchuk (personal communication, February 2023).

Table 6 below describes each stream.

Table 6: Description of information flows

№	Source	Reciever	Stream description
1	Card processing center	SAS ESP	Card processing event
1.1	SAS ESP	Card processing center	Decision whether to conduct/reject the operation in accordance with the triggered monitoring rules

To be continued

Table 6: Description of information flows (cont.)

2	SAS ESP	Automated banking system	Request to change card status
2.2	Automated banking system	SAS ESP	Message showing the request's status to change the card status
3	RBS channel of individuals and legal entities	SAS ESP	A message from RBS revealing non-financial information about the client. For example, registration in RBS, password change, establishment of a new representative for legal entities
4	RBS channel of individuals and legal entities	SAS ESP	A message from RBS revealing financial information about the client. For example, payments, transfers, opening and closing a deposit, etc.
4.1	SAS ESP	RBS channel of individuals and legal entities	Decision to conduct/suspend/reject the operation
5	SAS ESP	RBS channel of individuals and legal entities	Request to block/unblock access to RBS
5.1	RBS channel of individuals and legal entities	SAS ESP	Message with RBS blocking status
6	CRM system	SAS ESP	Notifications about changes in client's information/about completed requests of client's appeals to the bank
7	SAS ESP	SAS VI	Request for an alert on a suspicious transaction
7.1	SAS VI	SAS ESP	Message with the alert's status
8	SAS VI	SAS ESP	Request to block the card
9	SAS VI	SAS ESP	Request to block access to RBS
10	SAS ESP	Anti-fraud system's database	All events in SAS ESP (1 - 9) are being recorded to the anti-fraud system's database

To be continued

Table 6: Description of information flows (cont.)

11	Anti-fraud system's database	CDW	The data about ESP system events is exported to a data warehouse to calculate aggregated customer information. For example, the remain balance on the client's accounts.
12	CDW	Data mart	Based on the data from CDW data mart is formed for the anti-fraud system
13	Data mart	Anti-fraud system's database	Updated data from the data warehouse is loaded into the anti-fraud system's database, for example, information about new clients, terminals, etc., as well as calculated aggregated values
14	Anti-fraud system's database	SAS ESP	Information required for operations online verification is loaded into the RAM of the ESP and the database
15	Anti-fraud system's database	API of the financial CERT	A generated report on detected transactions that were performed without the client's consent is sent to the API of the financial CERT
16	API of the financial CERT	Anti-fraud system's database	Loading feeds of financial CERT into the database for further feeds usage in online verification process, as well as displaying the presence of a client/client's operations details in feeds in the SAS VI interface
17	SAS VI	Anti-fraud system's database	Transactions made without the client's consent are marked in SAS VI (the ones that must be sent to financial CERT). Information about these marks is stored in the anti-fraud system's database to generate a report on detected fraudulent transactions

Source: own work based on Andrey Pilipchuk (personal communication, February 2023).

The process of verifying the operation and the components of informational interaction have been studied. Based on this, the top-level structure of the SAS ESP (which is the information system that ensures the execution of the process and is part of the SAS Antifraud package) functional blocks was discussed with a representative of the bank.

Therefore, the structure consists of the following blocks:

1) Process steps

- Sending a request to carry out an operation;
- Preliminary processing the message;
- Checking the operation according to anti-fraud rules;
- Aggregating results of this check;
- Sending a response to a request with the status "Carry out/Reject/Suspend";
- Forming investigation;
- Forming a request to block the client;

– Carrying out/Rejecting/Suspending the operation;
– Executing a request to block a client.

2) Components of the architecture that are involved in the process of online verification of the operation:

– Processing center;
– Client RBS channel;
– SAS ESP;
– SAS VI;
– Automated banking system ABS.

3) Functional blocks of the anti-fraud system can be found in table 7:

Table 7: Functional blocks of the anti-fraud system

Process step	**Description of the anti-fraud system functional block**
Preliminary processing the message	Enrichment of card transactions information
	Enrichment of Operation Information in RBS
Checking the operation according to anti-fraud rules	Checking card transactions according to the anti-fraud rules
	Checking card transactions in RBS
	Checking card transactions and in RBS according to the anti-fraud rules
Aggregating results of the check	Forming the result of checking the operation based on the work of anti-fraud scripts
Sending a response to a request with the status "Carry out/Reject/Suspend"	Forming a response to a request for a card transaction
	Forming a response to a request for an operation in RBS
Forming investigation	Forming an alert based on the results of checking an operation in SAS VI
Forming a request to block the client	Forming a request to block the client's card in the Bank's ABS
	Forming a request to block client access to the RBS

Source: own work.

3.2 Further optimization steps

However, after starting the optimization process with replacing the current IS with SAS Antifraud, further on there can be indicated several possible ways to improve the accuracy of the anti-fraud system in the process of checking operations. Based on this research and discussions with the bank representative, the author identified some limitations that might appear and thought of possible ways to improve its accuracy. These ideas were also shared with the bank representative.

The suggestions might be the following:

- taking into consideration in the anti-fraud rules data about the devices that the client uses;
- taking into consideration in the anti-fraud rules data about the account to which the client transfers funds;
- taking into consideration in the anti-fraud rules information about the behavior of the client within the current session in the mobile or Internet bank. For example, the method of entering a login and password, moving the mouse, the number of attempts to enter the second identification factor;
- implementing a mechanism to prevent repeated activations of the anti-fraud system if the client confirms the operation;

The first three listed improvement ways refer to the use of information about a typical customer profile when verifying transactions, which is formed based on the history of customer transactions and non-financial activity over a long period of time. It is assumed that comparing the current operation of the client with his usual behavior pattern will reduce the number of false positives, as well as increase the level of fraud detection.

3.2.1 Requirements' formation for the analytical model of using the client's profile in SAS Antifraud system in the process of countering fraud

Utilizing data on the financial and non-financial the customer activity throughout a prolonged time (also known as profiles of standard buyer behavior) can become one of the methods for enhancing the effectiveness of the operational verification module. This could be among the methods to enhance the performance. The traditional anti-fraud technique, in which the current transaction is evaluated against pre-configured criteria for identifying particular fraudulent methods, is less effective for detecting fraudulent conduct than comparing a client's current behavior to their regular behavior. This is because the conventional anti-fraud strategy focuses on determining particular illegal strategies. The steps in preventing bank fraud may be summarized in the following requirement specification for the data and an analytical model that underpins creating a customer profile.

To form these criteria the author used information from an interview with bank X representative and conducted research on the types of fraud that the bank is facing, the data

that the bank collects on its clients, and the capabilities of the SAS Antifraud system. Based on this research, key features of the client's profile were identified that are relevant to detecting and preventing fraud, such as device usage patterns, transaction history, and demographic information. Finally, the specific requirements for the analytical model were determined, such as the types of statistical techniques to be used, the data processing and storage requirements, and the performance metrics to be tracked.

Firstly, the author identified the purpose of the client profile and the specific data points that would be most relevant in detecting fraud. Also, existing literature on the subject were reviewed and it was analyzed how similar algorithms have been developed in the past.

Then, a general idea of what the author wants to achieve was discussed with the expert in the field (bank X representative, a fraud detection professional) to get feedback on the feasibility and effectiveness of the proposed approach. Through this consultation, those requirements were refined and any potential challenges were identified that may arise in the development process. Afterwards, the list was shown to the bank representative for approval and his comments were taken into account.

Summing up, the process of developing requirements involved a combination of research, analysis, and consultation with the expert in the field to ensure that this approach is effective, feasible, and meets the specific needs of the anti-fraud system.

Requirements for the logical components of the model

The following data has to be integrated in the customer profile that is utilized in the process of preventing fraud:

- a record of the customer's authorized accounts where money has been sent;
- list of known and reliable contact information to whom the customer has sent money;
- a list of the card numbers that the customer may trust and to whom they have sent money;
- a catalogue of the client devices that may be trusted;
- average numbers of debit transactions carried out each day, each week, and each month, broken out by transaction type;
- a standard method for the user to submit their username and password into the channel (either "Copy - paste" or manually typing in the codes);
- routes of operation that are standard for the customer (telephone/mobile/Internet banking).

Requirements for the process of developing client profile using the algorithm

The following method must be followed while building the individual components of the client profile:

1. A list of trustworthy customer accounts. While compiling it, the date of the customer's first credit transfer to such an account, as well as the existence of a verified operation with this account have to be considered. If the customer received a warning about the operations from the device, the anti-fraud officer who examined the warning subsequently contacted the client, and together they validated the transaction, then this operation is deemed confirmed. Calls going out and in both have the potential for an operation confirmation. It is suggested that a user account should be regarded as trustworthy if the account's most recent transaction date is more than or equal to fourteen days in the past and the user account was validated during an incoming phone conversation.
2. A list of telephone numbers which a client used to request RBS device transfers. It is suggested the computation to be carried out like the one described in step 1.
3. A list of the customer's most reliable payment cards which they use for money transferring. It is suggested the computation to be carried out like the one described in step 1.
4. A list of trusted client devices. While doing calculations, the following variables and factors have to be considered:

– Amount of persons who have used the device;
– The occurrence of the customer uses this device;
– The frequency and value of the customer's activities from this device;
– How long the customer has been using it;
– This device has to have transactions verified by the customer.

In order to determine whether or not the client’s device can be trustworthy, a special algorithm has been developed. The logical "AND" operator is used to integrate each of the following conditions:

– The number of people logging into RBS using the device is 1;
– The very first input in the customer’s RBS that was made from this device occurred more than two months ago;
– The customer has used this device to access RBS on at least three separate occasions during the previous three months;
– The customer has already validated transactions made from this device more than seven days ago.

5. The average number of financial transactions that take place each day, each week, and each month. It is suggested that the following categories should be used to compute the average amounts of successful consumer debit transactions:

– operational issues;
– money transactions in the RBS.

6. A usual method client uses to input their username and password when they access a channel. They can be manual or using the copy-past technique. Non-monetary events, such as the event of entering the RBS, are received by the anti-fraud system through the RBS channels. It is recommended to calculate the share for each login method over the preceding six months in order to identify which data input technique is common for a customer and what proportion of the customer's RBS logins are performed using that approach. It is recommended that how the login is entered and the way in which the password is entered with maximum shares should both be deemed standard for the client. Due to the fact that a share of 0.49, for example, cannot be regarded as important, the share of inputs must also be included in the client profile. This is because the customer can type in the username and password in many different ways with roughly the same frequency.

In order to be more precise, these formulas can be used (every value is calculated for the period of last half of year):

- share of client logins to RBS using the method X for logging in = number of client logins to RBS using the method X for logging in / total number of client logins to RBS;
- share of client logins to RBS using the method Y for entering password = number of client logins to RBS using the method Y for entering password / total number of client logins to RBS;

In that case, the way of entering a login or password can be counted as usual if the share is over 0,8.

7. Common channels client uses. Customers complete their financial operations using various channels, including mobile/Internet/telephone banking. It is recommended that the share of the customer's actions in each channel over the previous half of a year is computed to identify which of the channels is more preferrable and thus standard for the client. It has been suggested that the channel with the highest share should represent the customer. In addition, the value of the shares has to be included in the customer profile as well.

In order to be more precise, these formulas can be used (every value is calculated for the period of last half of year):

- share of client transactions in RBS that are performed in the Z type channel = number of client transactions in RBS that are performed in the Z type channel / total number of client transactions;

In that case, the way of entering a login or password can be counted as usual if the share is over 0,8.

The following are the non-functional criteria that must be met in order to apply the analytical model:

- To determine the components of a customer's profile, the anti-fraud system database must be queried for data on the customer's transaction history over the last six months.
- At the time of checking the transaction in the anti-fraud system, the delay of no more than 3 minutes in updating data in the profile is allowed in the current client;
- If the anti-fraud system faces a bug, the existing customer profile must be computed and submitted to the system within three minutes of its restoration.
- The validation of the model needs to be performed using the information collected by the system for the first three months of a testing year.

3.2.2 Description of the formed analytical model of the client profile in the anti-fraud system

As part of the anti-fraud system optimization process, the importance of creating a client profile using an algorithm has been recognized to improve the accuracy of fraud detection. To achieve this, the author has researched different algorithms and analyzed their potential effectiveness in creating a comprehensive client profile. Based on this analysis, the author developed a description of the analytical model that would be used to create the client profile in the anti-fraud system. Of course, information received from the bank X representative was used too, as well as his comments regarding the formed analytical model were taken into account.

Operations that the client performs must not be suspended or rejected by the anti-fraud system if one of the following conditions is met:

- the operation is performed using a reliable device;
- the operation is performed using trusted bank details (account number, bank card, phone number).

It is assumed that eliminating these anti-fraud system’s responses can reduce the overall number of false positives. Operations that the client performs must be suspended or rejected by the anti-fraud system if one of the following conditions is met:

- the operation is not carried out using a reliable device;
- the method the client is entering the login or password tends to be atypical for him;
- the transaction channel is not usual for the client.

At the same time, for the latter two facts, the client's personal thresholds for the sum of a transaction should be considered. However, implementation of the thresholds is outside the scope of this study. To realize this technique, it is needed to have information about the following attributes about each client:

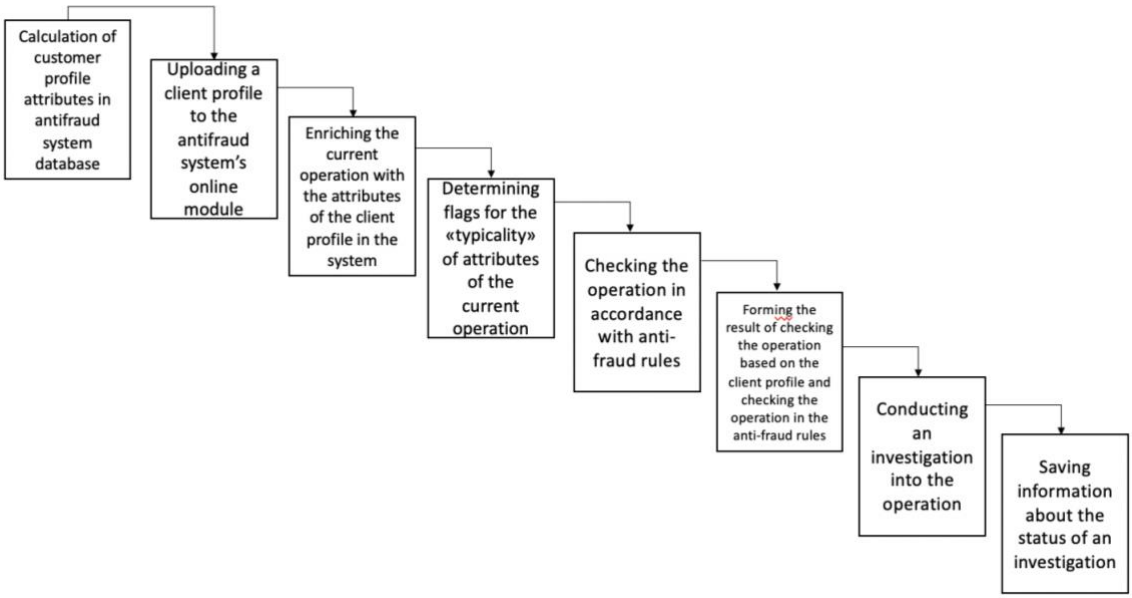
- client ID;
- listing of trusted accounts/card numbers/phone numbers/devices;

– data about the typical method of entering login/password;
– data about the typical operation channel.

3.2.3 Description of the to-be process of implementing the formed model using SAS Antifraud

As for the process of implementing the formed model using SAS Antifraud, the author came up with a description based on this research and understanding of the system's capabilities. The author reviewed the documentation and technical specifications of SAS Antifraud and analyzed its features and functionalities. Figure 10 shows the algorithm of the client profile model in the anti-fraud system. The left side of the diagram lists the steps in the process of using the client profile, and the right side shows a flowchart of the information model operation algorithm.

Figure 11: The algorithm for creating the client profile model in the anti-fraud system



Source: own work.

The explanation of the logical steps for implementing the model is the following:

1. First it is needed to calculate the attributes required to form a client profile in the anti-fraud system's database based on historical data on the financial and non-financial activity of the client. Calculation is carried out recurrently after a set timing.
2. Secondly, it is needed to load the calculated values into the online module. Loading of newly calculated values is carried out recurrently after a set timing.
3. Thirdly, it is needed to enrich the current operation with information from the client's profile. The profile is determined based on the client ID.

4. Regarding the operational attributes, it is needed to determine whether they are typical for the client or not. This information is taken into consideration when forming the overall score of a risky transaction: factors that are reducing risk (trusted device, trusted details of the transaction), as well as factors that are increasing risk (an atypical way for a user to enter a login and/or password, an atypical transaction channel).
5. Then, it is needed to check the operation in accordance with the anti-fraud rules. The result of checking the operation in the scenario is taken into consideration when forming the risk operation score.
6. Afterwards, there is a formation of the result of checking the operation in accordance with the client profile and the results of the anti-fraud rules. If the score of a risky operation exceeds the threshold value, then the operation is rejected or suspended, otherwise it is approved by the anti-fraud system. Information about the client's operation is stored in the anti-fraud system's database.
7. Then, the investigation is conducted. If the system generated an alert, the incident is being investigated. According to the outcomes of the investigation, the operation is either confirmed or not confirmed by the client. A transaction confirmed by the client, which was recognized by the anti-fraud system as fraudulent, indicates the presence of a false positive anti-fraud system.
8. Finally, there is a step of obtaining information about the alert status and adding this information to the database. The result of the incident investigation in the system is transmitted to the anti-fraud system's online module. Information about the result of the investigation is stored in the anti-fraud system's database.

3.3 Assessment of expected business effects of the optimized anti-fraud process

If the bank decides to implement the proposed optimization path, then it will be necessary to calculate the quantitative characteristics of the anti-fraud system using the developed model, demonstrating an increase in the quality of the system. These quantitative characteristics include:

- volume of saved customer funds;
- the number of clients whose transactions were not suspended due to incorrect operation of the anti-fraud system.

As it has been mentioned earlier, the decrease in customer loyalty due to the rejection or suspension of their transactions due to the incorrect operation of the antifraud is a serious problem for the bank. When using the developed model, customers would not have problems with the implementation of operations compared to the work of antifraud without using the model. The change in the transactional activity of the bank's customers in each quarter of the year is insignificant, therefore, the results obtained can be considered as the expected effect of the implementation of the model in the following quarters.

The assessment of expected business effects of the optimized anti-fraud process can be done by considering various factors such as:

- Reduction in fraud losses: the optimized anti-fraud process should lead to a reduction in fraud losses, which can be measured by comparing the historical fraud losses to the new fraud loss figures after implementing the optimized process. This reduction in fraud losses can have a positive effect on the operation of the business.
- Improved customer trust: customers are likely to trust a bank or financial institution more if they feel that their money is safe from fraud. Implementing an optimized anti-fraud process can help in building customer trust, leading to improved customer loyalty, retention, and acquisition.
- Reduction in false positives: false positives are a major concern in the anti-fraud process, as they can lead to delays in processing legitimate transactions and negatively impact customer experience. An optimized anti-fraud process should help reduce false positives, leading to better customer satisfaction and operational efficiency.
- Increased operational efficiency: an optimized anti-fraud process can lead to increased operational efficiency by reducing the need for manual reviews, improving the accuracy of fraud detection, and streamlining the overall fraud management process. As a result, there can be savings in costs and enhanced productivity.
- Compliance with regulatory requirements: banks and financial institutions are subject to various regulatory requirements related to fraud detection and prevention. Implementing an optimized anti-fraud process can help in ensuring compliance with these regulations and avoiding penalties.

Overall, the optimized anti-fraud process is expected to have a positive impact on the business by reducing fraud losses, improving customer trust and satisfaction, increasing operational efficiency, and ensuring compliance with regulatory requirements.

Summing up, this section offers a review of the Bank X everyday activities, as well as a description of the high-level architecture of the information systems used by the bank. The amount of details regarding this information system is suitable for study purposes within the context of this thesis. In this part, an analysis of the anti-fraud process was performed, a description of the information flows that occurred throughout the process was presented, and the top-level description of the system of the functional blocks of the SAS ESP that corresponded to the anti-fraud process in the bank was carried out. Also, the anti-fraud procedure was analyzed, which included the following:

- a list of the system's holdups was compiled;
- a description of the method used to compute the performance measures of the anti-fraud system was provided based on the information got from Bank X’s representative, and calculations of those metrics themselves were analyzed. The statistic used to measure the proportion of suspicious purchases that go unnoticed is the missed fraud cases, and its current value is 0.0000183. The value of the false-positive frauds indicator, which

describes the percentage of false positives produced by the system, is equal to 0.72 (which indicates that around 70% of the positives generated by the anti-fraud system are incorrect).

It has been suggested by the author that the system's reliability might be improved by implementing SAS Antifraud system, as well as using past information on the customer's financial and non-financial activity while verifying the operation (also known as a standard/usual client behavior profile).

There were defined both functional and non-functional criteria for an informational and analytic model to employ a client profile to prevent and detect fraudulent activity. In addition to applying the results gained during the research of existing fraud schemes, laws in this area, and the function of the most powerful anti-fraud systems now readily available on the market, the criteria were defined based on the business statement provided by the representative from Bank X.

Therefore, the aim of exploring the procedure of combating fraud in a large Russian bank and processing requirements for an information-analytical model that supports the antifraud procedure was accomplished within the scope of this thesis part. This effort was completed in order to fulfill the aim of this chapter.

CONCLUSION

Implementing SAS antifraud systems can be an effective way to optimize the process of countering fraud in a financial institution. The research has shown that SAS antifraud systems are capable of detecting fraudulent activities with high accuracy and speed, thereby reducing the risk of financial losses and reputational damage for the institution.

Moreover, SAS antifraud systems can help financial institutions to comply with regulatory requirements related to fraud detection and prevention, reducing the risk of penalties and legal liabilities. With improved fraud detection and prevention capabilities, the financial institution can also enhance its operational efficiency, leading to significant cost savings and increased productivity.

Overall, the implementation of SAS antifraud systems can result in a win-win situation for financial institutions and their customers, providing improved security and trust, while at the same time, optimizing the institution's fraud management process.

As the outcome of the study, the following results have been achieved:

– international and domestic aspects of the activities of financial institutions in the framework of the risk management process and the legal framework in this area were studied;

- the analysis of statistical data on stolen funds in Russia, the USA and the countries of the single euro payments area was carried out. Based on the found-out indicators, it can be concluded that the measures that are currently being implemented to combat fraud are not enough. New methods need to be developed to track and prevent fraud in real time;
- actual fraud schemes were studied. Based on the analysis of the schemes, the problems associated with fraud were identified, proposals for their solution and requirements for information systems that implement them were formed;
- a typical process of countering fraud in financial institutions using information and analytical systems was studied. The author identified four areas of activity: countering internal fraud, transactional fraud, interaction with the regulator, information security. For the antifraud process to be effective, all areas must be developed in parallel, since ignoring one of them can make work in other areas useless;
- a comparative analysis of the most popular anti-fraud systems was carried out in terms of their functionality and technical aspects of implementation and operation. The criteria on the basis of which the comparison was carried out were developed, among other things, in the analysis of current fraud schemes;
- a study of the anti-fraud process in a large Russian bank was carried out, the bottlenecks of the process were identified and proposals were made on how to improve the quality of the process based on formalized metrics;
- requirements for the information-analytical model that provides the anti-fraud process have been developed. The model implies the use of information about the transactional activity of the bank's client over a long period of time and the comparison of the parameters of the current operation with the typical behavior of the client;
- an information and analytical model was developed for using a profile of typical client behavior to ensure the required quality of the anti-fraud process. The paper describes the algorithm of the model.

Thus, the research solves all the tasks set and the goals of the study were achieved. The developed information and analytical model for using the client profile has the potential for development. In particular, the algorithm for calculating the components of the client profile should be updated based on actual data on the quality of the anti-fraud system. At the same time, the results of the model operation should be available for analysis in the context of the components of the client profile in order to make changes to the algorithm for their calculation. Thus, due to automated monitoring of the quality of the model and making changes, we get a feedback control loop.

REFERENCE LIST

1. Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I. (2020). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science, 3*.
2. Al-Shiha, A. M. O., Nordin, M. N. & Yusoff, R. M. (2018). Money Laundering and Terrorism Financing through Digital Payment Systems: A Review of the Literature. *International Journal of Supply Chain Management (IJSCM), 7* (6), 111 – 118.
3. Analytics Software & Solutions. (n.d.). *SAS Fraud Management*. https://www.sas.com/en_si/software/fraud-management.html.
4. 360quadrants Agency. 2022. *Best fraud detection software*. https://www.360quadrants.com/software/fraud-detection-and-prevention-solutions.
5. Ashbaugh-Skaife, H. & Sanchez, M. (2020). The Role of Technology in the Detection and Prevention of Financial Statement Fraud: A Review of the Literature. *Journal of Accounting Literature, 44*, 23 – 37.
6. Bank of Russia. (2022). *Overview of transactions not authorized by customers of financial institutions in 2021*. https://www.cbr.ru/eng/analytics/ib/operations_survey/2021.
7. Bank of Russia. (2021). *Overview of transactions not authorized by customers of financial institutions in 2020*. http://www.cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf
8. Bank of Russia. (n.d.). *Federal Law: On the Central Bank of the Russian Federation (Bank of Russia)*. https://www.cbr.ru/Content/Document/File/95793/law_cb_e.pdf.
9. Bank of Russia. (2014). *Bank of Russia Standard: Maintenance of information security of the Russian banking system organisations*. http://www.cbr.ru/content/document/file/51218/st-12-14_en.pdf.
10. Bank of Russia. (2019). *Guidelines for the advancement of information security in the financial sector for 2019–2021*. http://www.cbr.ru/content/document/file/103460/onrib_2021_e.pdf.
11. Bao, Y., Liang, L. & Zhao, H. (2019). Big Data Analytics for Fraud Detection in Banking: A Comprehensive Review. *Journal of Financial Services Research, 55*, 163 – 185.
12. Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management, 2020*, 1 – 10.
13. Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N. & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security, 2020*, 15 – 19.
14. Bhargava, B., Srinivasan, A. & Dave, M. (2019). A Framework for Detecting and Preventing Data Leakage in Enterprises. *Journal of Internet Commerce, 18*(2), 152-169.
15. Bhattacharya, S., Goswami, S. (2019). *Bank Fraud: Types, Detection and Prevention. Journal of Financial Crime, 26*, 109 – 128.
16. Bhattacharyya, S., Sha, S. & Tharakunnel, K. (2011). Data mining for credit card fraud: a comparative study. *Decision Support Systems, 50*, 602 – 613.

17. Bialek, A., Chmielewski, M. & Kulesza, K. (2020). The Process of Countering Transactional Fraud in Financial Institutions. *Risk in Contemporary Economy, 2* (2), 119 – 130.
18. Binwahlan, M. T., Al-Shabandar, M. & Al-Betar, M. (2018). Detecting Fraudulent Online Banking Transactions Using Machine Learning Techniques. *Journal of Information Security and Applications, 41, 102 – 117.*
19. Bottomline Technologies. (2021). *Treasury Fraud and Controls Research Report.* https://www.bottomline.com/uk/resources/2021-treasury-fraud-and-controls-research-report.
20. Cárdenas, R., Soto, R., Montenegro, S., M. E. Cortés, M. E. & Montenegro, D. (2018). Analyzing transactional fraud in the banking sector using machine learning techniques. *Expert Systems with Applications, 94,* 54 – 65.
21. Chang, C.-L., Lin, Y.-M., & Lin, C.-Y. (2019). A Framework of Data Leakage Prevention System Based on Machine Learning Techniques. *International Journal of Innovative Computing, Information and Control, 15*(2), 635 – 651.
22. Chen, H., Chen, D. (2020). Design and implementation of anti-fraud system for banks based on distributed computing. *2nd International Conference on Computing and Artificial Intelligence, ICCAI* (2020), 35 – 40.
23. Curtin, L. & Lazowski, M. (2019). The European Anti-Fraud Office (OLAF) and the Protection of the EU Financial Interests: An Overview of its Role, Structure and Procedures. *European Public Law journal, 25*(1), 49 – 74.
24. Davenport, J. & Milburn, S. (2021). A Comparative Study of Non-Functional Requirements for Anti-Fraud Systems. *Proceedings of the International Conference on Information Systems Security, 17th edition.*
25. Domashova, J. & Zabelina, O. (2021). Detection of fraudulent transactions using SAS Viya machine learning algorithms. *Procedia Computer Science, 190,* 204 – 209.
26. Dorn, N., Huber, M., Van der Heijden, T. (2021). Typical Patterns of Behavior of Fraudsters: Evidence from Financial Services Providers. *Journal of Financial Services Research, 59*(1), 1 – 25.
27. Eni-Olorunda, O., Pappas, I., Karmakar, S. (2020). A Framework for Integrating Anti-fraud Systems in Banks. *International Journal of Bank Marketing, 38*(4).
28. European Central Bank. (2020). *Seventh report on card fraud.* https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html.
29. European Council, and Council of the European Union. (2020). *Fighting against money laundering and terrorist financing.* https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/.
30. European Payments Council. (2022). *Payment threads and Fraud Trends Report.* https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

31. FATF. (2023). *Outcomes FATF Plenary*. https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html
32. Federal Trade Commission. (2023). *Report on the stolen funds in the USA in year 2022.* https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.
33. Gallo, A. S., Lombardi, R., Lippi, F., Sabato, G. (2021). Current Fraudulent Schemes in the Banking Sector: Detection and Prevention Strategies. *Journal Sustainability, 13*(6), 1 – 23.
34. Gartner. (n.d.). Data Quality Solutions Reviews and Ratings. https://www.gartner.com/reviews/market/data-quality-solutions.
35. Gamage, M. (2019). Design and Implementation of a Real-Time Anti-Fraud System for Electronic Banking Transactions. *International Journal of Advanced Computer Science and Applications, 10*(11), 161 – 167.
36. Härle, P., Havas, A., Kremer, A., Rona, D. & Samandar, H. (2015). The future of bank risk management. *McKinsey Working Papers on Risk*, 6 – 24.
37. Haldorai, A., Chakraborty, A., Srinivasan, S. (2021). A Study of Data Masking Techniques and their Effectiveness in Protecting Sensitive Data. *Journal of Information Privacy and Security, 17*(2), 57 – 72.
38. Hussain, Z., Al-Khasawneh, A., Alsmadi, I. (2020). A Comprehensive Approach for Combating Internal Fraud in Financial Institutions: A Systematic Literature Review. *Journal of Financial Crime, 27*(3), 751 – 767.
39. Islam, M. M., R. Islam, R., Hossain, M. A. (2020). Machine Learning-based Anti-fraud System for e-Commerce Transactions: A Comparative Study. *23rd International Conference on Computer and Information Technology, 2020*, 1 – 6.
40. Jayaprakash, R. & Vetrivelan, Dr. P. (2019). Data Masking Techniques in Privacy Preservation - A Review. *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking, 2019*, 1 – 5.
41. Javelin. (2021). *Identity Fraud Study: Shifting Angles*. https://www.javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study.
42. Young, A., Jordon, A., Kratz, J., Wiberg, M. (2018). The State of European Tech 2018. *Atomico*, 124.
43. Jaksic M., Marinc M. (2018). Relationship Banking and Information Technology: The Role of Artificial Intelligence and Fintech. *SSRN Electronic Journal, 3059426*.
44. Jung, J.-K., Shin, Y.-J., Cho, S.-B. (2014). The study of current fraudulent schemes and the proposed solutions for anti-fraud systems. *Journal of Security Engineering, 11*(3), 131– 138.
45. Junger, M., Wang, V. & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science, 9*, 1– 15.
46. Karpoff, J. M. (2020). The future of financial fraud. *Journal of Corporate Finance*, 101694.

47. Kassem, M., Oueidat, M., Hage, G. (2021). Fraud Detection and Prevention Techniques in Banking Industry: A Systematic Literature Review. *Journal of Financial Crime, 28*(2), 593 – 608.
48. Kroll and the Ethisphere Institute. (2018). *Global Banking Fraud Survey*. https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2018
49. KPMG. (2020). *The multi-faced threat of fraud*. https://kpmg.com/dp/en/home/insights/2020/02/the-multi-faceted-threat-of-fraud.html
50. Lawson, P., Pearson, C. J., Crowson, A., Mayhorn, C. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics, 86*.
51. LexisNexis (2019). *True Cost of Fraud Study: Financial Services and Lending Edition*. https://risk.lexisnexis.com/-/media/files/financial%20services/research/lnrs_true-cost-of-fraud-financial-services-and-lending-2021_research.pdf.
52. Liao, L. & Yang, Y. (2018). Early warning of bank credit fraud based on logistic regression model. *International Journal of Hybrid Information Technology*, *11*(4), 19 – 28.
53. Lukonga, I. (2018). Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions. *International Monetary Fund's, WP/18/200*, 1 – 37.
54. McKinsey & Company. (2020). *The future of bank risk management*. https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/pdfs/the_future_of_bank_risk_management.ashx.
55. Modi, K., Dayma, R. (2017). Review on fraud detection methods in credit card transactions. *International Conference on Intelligent Computing and Control*, 1 – 5.
56. Mustafa, I. & Ghazali, S. (2021). A Hybrid Anti-Fraud Model for Financial Transactions Based on Deep Learning and Fuzzy Logic. *IEEE Access, 9*, 42020 – 42037.
57. Mwema, C., Mamboleo, G. (2018). A framework for developing an anti-fraud system for banks. *Journal of Money Laundering Control*, *21*(3), 351 – 363.
58. Nilson. (2021). *Card Fraud Worldwide*. https://nilsonreport.com/upload/content_promo/NilsonReport_Issue1209.pdf
59. Nweke, H. F., Asogwa, B. E. (2020). A framework for integrating anti-fraud systems in banks. *International Journal of Bank Marketing, 38*(3), 605 – 620.
60. Osei-Assibey, M., Kwarteng, K. (2020). The Impact of Internal Controls on Fraud Detection in Financial Institutions: A Study of Selected Banks in Ghana. *International Journal of Finance and Accounting, 9*(4), 177 – 186.
61. Prasad, A. V. S., Venugopal, K. R. (2020). Fraud Detection in Banking Systems: A Review. *International Journal of Computer Applications, 177*(1), 1 – 7.
62. PwC. (2022). *Protecting the perimeter: The rise of external fraud*. https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf
63. Ram, T., Acharya, K. (2021). Banking Frauds: Causes and Preventions. *International Journal of Advanced Research and Publications, 5*(7), 104 – 109.

64. SAS Institute. (n.d.). *Credit Risk Management.* https://www.sas.com/en_us/insights/risk-management/credit-risk-management.html.
65. SAS. (n.d.). *SAS Intelligent Decisioning.* https://www.sas.com/en_si/software/intelligent-decisioning.html.
66. SAS Institute. *Product overview: SAS Intelligent Decisioning.* https://video.sas.com/detail/video/6052014281001/product-overview:-sas-intelligent-decisioning.
67. SAS. (n.d.). *SAS Real-Time Decision Manager*. https://support.sas.com/en/software/real-time-decision-manager-support.html.
68. SAS. (n.d.). *SAS Visual Analytics.* https://www.sas.com/ru_ru/software/visual-analytics.html.
69. SAS. (2021). *Banking Fraud Survey.* https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/third-party-whitepapers/en/coalition-against-insurance-fraud-the-state-of-insurance-fraud-technology-105976.pdf
70. Sumsub. (2022). *Sumsub Identity Fraud Report.* https://sumsub.com/downloads/fraud_report_2022.pdf
71. The Eurasian group on combating money laundering and financing of terrorism (EAG). https://eurasiangroup.org/en.
72. Ullah, R., Akhtar, M. N. (2021). Combating internal fraud: A proactive approach. *Journal of Financial Crime, 28*(1), 140 – 155.
73. Votintseva, L. (2019). Digital transformation of Russian banking institutions: Assessments and prospects. *IOP Conference Series: Materials Science and Engineering, 2019*.
74. Waheedah O. I. & Branch, S. (2021). Financial Statement Fraud: Challenges and Technology Deployment in Fraud Detection. *International Journal of Business and Information, 16*, 147 – 162.
75. Walters, E. J. & van der Merwe, P. J. (2019). The Internal Fraud Risk Management Process. *Journal of Financial Crime, 26*(3), 698 – 712.
76. West, J. & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Journal of Financial Crime, 23*(4), 781 – 802.
77. Pega. (2019). *Why banking needs to put service first.* https://www.pega.com/insights/resources/why-banking-needs-put-service-first
78. Xiaoqian, Z., Xiang, A., Zidi, Q., Yanpeng, C., Yang, L., Qing, H., Jianping L. (2021). Intelligent financial fraud detection practices in post-pandemic era. *The Innovation, 2*(4).
79. Xue, W., Turner, M. J., Zhang, H. (2021). Combating financial fraud: The role of internal controls and risk management. *Journal of Financial Crime, 28*(1), 128 – 141.
80. Zhang, D., Yuan, X. (2020). An Automated Fraud Detection System for the Insurance Industry Using SAS® Enterprise MinerTM. *Proceedings of the SAS Global Forum*.

81. Zhou, Q., Zhang, Y., Wang, T. (2021). Social Engineering: A Review and Future Research Directions. IEEE Transactions on Information Forensics and Security, 16, 2957 – 2972.

APPENDICES

Appendix 1: Povzetek (Summary in Slovene language)

Porast inovacijskega razvoja v bančnem sektorju je tesno povezan z vse večjo digitalizacijo v globalnem gospodarstvu. Ena glavnih težav bank je ta, da se je v zadnjih letih močno povečala konkurenca na finančnem trgu. Poslovanje v razmerah velike konkurence in spreminjajočih se preferenc uporabnikov sili akterje na trgu, da si prizadevajo vsak dan narediti nekaj novega, s čimer bi se razlikovali od svojih tekmecev in ne le ohranili, temveč tudi povečali število svojih strank. Nove tehnologije bankam dajejo priložnost bistveno spremeniti obdelavo plačil, izboljšajo regulativni nadzor, upravljanje tveganj, zaposlovanje, razvoj novih produktov ter način interakcije z njihovimi sedanjimi in bodočimi strankami. Tako je namreč potrebno manj posredovanja zaposlenih v procesih, zaradi česar so ti bolj stroškovno učinkoviti, natančni in neodvisni od človeka. S kompleksnostjo tehnologij in njihovo razpoložljivostjo pa se hkrati povečuje tudi ranljivost uporabe digitalnih storitev. V takšnih pogojih se vedno več pojavljajo goljufije, tudi v kreditnem in bančnem sektorju. Goljufije v bančništvu so zapleten in večplasten pojav, na katerega vplivajo različni dejavniki, vključno z gospodarskimi razmerami, organizacijsko kulturo in tehnološkim napredkom. V zvezi s tem postaja izvajanje ukrepov proti goljufijam v finančnih institucijah eno od najpomembnejših in najbolj relevantnih področij na področju upravljanja tveganj.

Namen magistrske naloge je bil raziskati možnosti uporabe sistemov SAS za boj proti goljufijam in podati predloge, kako bi bilo mogoče tak sistem implementirati v proces upravljanja tveganj v veliki ruski banki, z namenom izboljšanja in optimizacije procesov odkrivanja sumljivih transakcij ter podpore pri reševanju težav v boju proti goljufijam.

Cilji magistrske naloge so bili:

- preučiti mednarodne vidike delovanja finančnih institucij v okviru postopkov upravljanja tveganj in raziskati pravne prakse na tem področju;
- poiskati in analizirati statistične podatke v zvezi z odtujenimi sredstvi in najpomembnejšimi prevarantskimi shemami;
- raziskati tipičen postopek boja proti goljufijam v finančnih institucijah, ki uporabljajo informacijske in analitične sisteme;
- poiskati najbolj priljubljene sisteme za boj proti goljufijam in jih primerjati glede na njihovo funkcionalnost ter tehnične vidike izvajanja in delovanja;
- izvesti pregled obstoječega procesa boja proti goljufijam v izbrani banki;
- ugotoviti slabosti sedanjega procesa in predlagati načine za izboljšave;
- pripraviti zahteve za analitični model, na podlagi katerih bi bilo mogoče optimizirati proces boja proti goljufijam;
- predlagati optimiziran poslovni proces z uporabo sistemov SAS za boj proti goljufijam.

Celovitost te študije je bila zagotovljena z metodami kot so analiza, primerjava in modeliranje procesov, ki so omogočile podrobno analizo procesa boja proti goljufijam v izbrani banki, da bi predlagali načine za izboljšanje in optimizacijo.

Kot viri informacij so bili uporabljeni primarni in sekundarni viri, kot so regulativni pravni akti, gradiva znanstvenih člankov na temo boja proti goljufijam, gradiva s konferenc na tem področju ter gradiva organizacijske enote banke, centra za spremljanje in odzivanje na računalniške napade v finančnem sektorju. Poleg tega sem intervjuvala več predstavnikov banke, katerih delo je povezano z informacijsko tehnologijo in upravljanjem informacijske varnosti, vlaganjem v tehnološke inovacije in partnerstva ter nadzorom nad tehnološkimi tveganji in upravljanjem kibernetske varnosti v banki. Njihovi predlogi so bili tudi upoštevani pri pripravi naloge. Zaradi ohranjanja zaupnosti podatkov, kot je bilo zahtevano s strani predstavnikov banke, so bili ime banke in druga identifikacijska dejstva spremenjeni.

Na podlagi raziskave sem ugotovila, da se da s pomočjo sistemov SAS za boj proti goljufijam zelo natančno in hitro odkrivati prevarantske dejavnosti ter tako zmanjšati tveganje finančnih izgub in škode ugledu institucije. Poleg tega lahko sistemi SAS proti goljufijam finančnim institucijam pomagajo pri izpolnjevanju regulativnih zahtev, povezanih z odkrivanjem in preprečevanjem goljufij, s čimer se zmanjša tveganje za kazni in pravne obveznosti. Z izboljšanimi zmogljivostmi za odkrivanje in preprečevanje goljufij lahko finančna institucija poveča tudi svojo operativno učinkovitost, kar vodi k znatnim prihrankom stroškov in večji produktivnosti.

V sklopu magistrske naloge je bilo opravljeno naslednje:

- Preučeni so bili mednarodni in domači vidiki dejavnosti finančnih institucij v okviru procesa upravljanja tveganj ter pravni okvir na tem področju.
- Opravljena je bila analiza statističnih podatkov o odtujenih sredstvih v Rusiji, ZDA in državah enotnega območja plačil v eurih. Na podlagi ugotovljenih kazalnikov je mogoče sklepati, da ukrepi, ki se trenutno izvajajo za boj proti goljufijam, niso zadostni. Razviti je treba nove metode za sledenje in preprečevanje goljufij v realnem času.
- Preučene so bile dejanske sheme goljufij. Na podlagi analize shem so bile ugotovljene težave, povezane z goljufijami, oblikovani so bili predlogi za njihovo reševanje in zahteve za informacijske sisteme, ki jih izvajajo.
- Proučen je bil tipičen postopek boja proti goljufijam v finančnih institucijah z uporabo informacijskih in analitičnih sistemov. Pri tem sem opredelila štiri področja delovanja: preprečevanje notranjih goljufij, transakcijske goljufije, interakcija z regulatorjem in informacijska varnost. Da bi bil proces boja proti goljufijam učinkovit, je treba vsa področja razvijati vzporedno, saj je lahko zaradi ignoriranja enega od njih delo na drugih področjih nekoristno.
- Opravljena je bila primerjalna analiza najbolj priljubljenih sistemov za boj proti goljufijam glede na njihovo funkcionalnost ter tehnične vidike izvajanja in delovanja. Merila, na podlagi katerih je bila opravljena primerjava, so bila med drugim oblikovana pri analizi sedanjih sistemov za preprečevanje goljufij.

- Izvedena je bila analiza procesa boja proti goljufijam v veliki ruski banki, opredeljena so bila ozka grla procesa in podani predlogi, kako izboljšati kakovost procesa na podlagi formaliziranih metrik.
- Definirane so bile zahteve za informacijsko-analitični model, ki zagotavlja proces boja proti goljufijam. Model predvideva uporabo informacij o transakcijski dejavnosti stranke banke v daljšem časovnem obdobju in primerjavo parametrov trenutnega poslovanja s tipičnim vedenjem stranke.
- Razvit je bil informacijski in analitični model za uporabo profila tipičnega vedenja stranke za zagotavljanje zahtevane kakovosti procesa boja proti goljufijam. V nalogi je opisan algoritem modela.

Če povzamemo, so bile z raziskavo rešene vse zastavljene naloge in doseženi cilji raziskave.

Appendix 2: Online questionnaire with Andrey Pilipchuk

Andrey Pilipchuk, IT department (contacts: pilipchuk.a.1987@gmail.com)

(Q) Can you tell me about your background and experience in fraud prevention? How did you become interested in this field?

(A) I have been working in fraud prevention for over 10 years, and I have a background in finance and law enforcement. I became interested in this field because I saw the devastating impact that fraud can have on individuals and businesses. I am passionate about using my skills and expertise to protect our customers and the bank from fraudulent activity.

(Q) What are some common types of fraud that you encounter in your role as an anti-fraud officer?

(A) Some common types of fraud we encounter include phishing scams, identity theft, credit card fraud, and check fraud. These can take many different forms and can be perpetrated by individuals or organized crime groups.

(Q) How do you stay up-to-date with the latest trends and techniques in fraud prevention?

(A) I attend industry conferences and training sessions, read industry publications, and participate in professional organizations related to fraud prevention. I also work closely with our IT and security teams to stay abreast of emerging threats and technology.

(Q) Can you describe the high-level architecture of the bank's information systems?

(A) Separate application databases are used to store historical information from the bank's systems. Upon collection, this information undergoes a number of transformations to standardize its structure and keys. During this process, the data is cleaned and checked for quality, while data consistency and integrity are ensured. Consequently, a corporate data warehouse (CDW) is created. This unified and standardized CDW data enables the development of various storefront consumer systems based on specific bank departments' business requests, such as BI or CRM systems, anti-fraud systems, and systems that monitor overdue debts for the Collection division.

The bank's architectural features relevant to the aims of this work are highlighted with green on the figure. Data required for the anti-fraud process enters the anti-fraud system to be verified and analyzed. Data about the system's operation is stored in the anti-fraud system's database and then undergoes the transformation procedure for being stored in CDW.

(Q) Can you walk me through the steps you take when investigating a fraud case? What tools and resources do you use?

(A) When investigating a fraud case, we start by gathering as much information as possible from the customer and any other sources. We use a variety of tools and resources, including fraud detection software Antifraud.Internet that is our main system for detecting all sorts of fraudalent activities. The steps include transaction monitoring, risk assessment, blocking fraudulent transactions; data analysis. Enlarged, fraudsters are filtered out at three levels. First, rough assessment rules are triggered: yes/no, allowed/not allowed, filters by black or white lists. Everything that is filtered out at this stage is passed to the machine learning component for saturation of the historical data storage and self-learning of the models. Then comes the rule-based filters - there are many of them, they are different, and I definitely cannot talk about all of them as this is a secret information but I will show you several . Finally, when the fraud machine is uncertain about which decision to make, the event is sent to the third level, where machine learning models are launched, which supplement the rule-based filters. Some types of events always undergo machine learning model testing to generate additional second-level rules.

(Q) Are the results of this system you get satisfactory to the bank?

(A) Not really. While the scheme is complex, the idea is simple. A set of data about a transaction, user type of authorization, etc. is receives, and the system processes it in the anti-fraud machine and gives a verdict - are there any fraudsters there or not. Obviously, there often happen mistakes. For example, the system flags legitimate transactions as fraudulent and blocks them, causing inconvenience and frustration to the customer. Or it sometimes fails to detect the real fraud and allows fraudulent transactions to go through.

(Q) Why does that happen?

(A) Because "Antifraud.Internet" is too straightforward, it depends too much on automated rules and algorithms. It does not take into account the gradations of individual transactions. It cannot be flexible, though this is very important in the modern world.

(Q) What problems can the bank face because of such failures?

(A) Usually that impacts financial losses and perhaps damage to the reputation, because we can lose clients’ trust.

(Q) Can you sum-up the system’s disadvantages?

(A) Those are inability to handle new types of fraud, too often false positives, inefficiency, difficulties with implementation, costs, low accuracy of fraud detection, insufficient protection against hacking.

(Q) What can be done to increase the quality of the antifraud system?

(A) The most obvious one is to decrease the number of false positives and to decrease the number of missed fraudulent transactions in the same time increasing the number of identified fraudulent transactions.

(Q) How do you work with other departments within the bank (such as legal, compliance, and risk management) to prevent and investigate fraud?

(A) Collaboration is key to preventing and investigating fraud. We work closely with legal, compliance, and risk management to ensure that our policies and procedures are effective and up-to-date. We also share information and insights to help identify and prevent fraudulent activity.

(Q) Have you ever encountered a particularly challenging or complex fraud case? How did you handle it?

(A) Yes, I have encountered many challenging and complex fraud cases over the years. In these situations, it's important to remain calm and focused, gather as much information as possible, and work closely with other experts and agencies. We also learn from each case and continually improve our fraud prevention and investigation techniques.

(Q) What steps does the bank take to educate customers about fraud prevention and protect their personal information?

(A) We offer educational resources and training to our customers on how to protect their personal information and avoid fraud. We also use a variety of security measures, such as encryption and multi-factor authentication, to protect our customers' data.

(Q) What are some emerging trends or technologies in fraud prevention that you are keeping an eye on?

(A) We are closely monitoring the use of artificial intelligence and machine learning in fraud.

(Q) Do you know any existing technologies that are being used in bank sphere to enable fraud monitoring?

(A) Yes, there are a few of them, for example IBM Safer Payments or SAS Fraud and Security Intelligence.

(Q) Can you maybe list their advantages and disadvantages?

(A) Well, for example, events in the IBM Safer Payments contain only a single level of information, without any further levels of sub-information within them. For example, consider an event that contains information about a financial transaction, such as the transaction amount, date, and location. If this event is "flat," it means that all of this information is contained within a single level and there are no further levels of sub-

information within it. Also, the interface, or the visual display and tools used for setting up rules in IBM Safer Payments Processes, cannot be modified or personalized according to the user's preferences or needs. It is a fixed interface that the user has to work with as it is designed by the software developers. The user cannot add or remove any features, change the layout or appearance, or adjust any settings related to the interface. The interface is set and cannot be altered by the user. For comparison, the NetReveal has a module with a pre-configured set of risk indicators, which are used to identify potential fraudulent activities or risks related to financial transactions. It also allows the users to customize and configure their own verification rules based on the bank's specific expertise and requirements. However, users cannot modify how the information is presented or displayed on the interface.

(Q) What about FICO Falcon Platform?

(A) As far as I know, it is only designed to monitor and analyze transactions that occur on the internet, such as online purchases, banking transactions, or other digital transactions. It is not capable of verifying physical card transactions. To verify physical card transactions, a separate system or process is needed. So it is not very convenient.