**Nikola Stefanović**
**Tamara Đalić** [1]
**Jovana Vesić**

# MANAGING CREDIT AND CARD FRAUD PHENOMENA IN THE BANKING SYSTEM OF THE REPUBLIC OF SERBIA

**Article info:**
Received 20.10.2022.
Accepted 20.08.2023.

UDC – 336:364-781.2
DOI – 10.24874/IJQR18.01-15

***Abstract:*** *The paper discusses an analysis of credit and card fraud phenomena identified by a multinational bank in the Republic of Serbia. The research aims to evaluate the effectiveness of existing systems and practices for managing fraud risks in the banking sector of the Republic of Serbia. It explores the potential impact of fraudulent activities on the credit and card processes, as well as risk management in the banking system during the period before, during, and after the Covid-19 pandemic, specifically from 2018 to 2022. The most significant research result provides a descriptive profile of potential fraud perpetrators in the banking sector. This can contribute to decision-makers in finance, managers, and analysts to better scrutinize the profiles of potential credit users. Recognizing early signs that indicate a person is likely to commit fraudulent acts allows banks to prevent potential fraud in a timely manner, thus averting possible financial losses.*

***Keywords:*** *banking risks, credit frauds, fraud perpetrator, credit card*

## 1. Introduction

The specificity of banking intermediation is reflected in risk assumption and its public nature (Knežević et al., 2021). The necessary qualitative determination of the term 'bank'is that it performs financial intermediation by assuming a certain risk (Đukić, 2003; Gogić, 2021). Both the operation and the organization of the bank are subordinated to it. Every uncertain fact in banking, as in other forms of economic activity, represents a risk (Milojević, 2016). When discussing risks in banking, this primarily refers to classical risks (Vesić et al., 2019), such as credit risk, liquidity risk, and interest rate risk. In addition to these risks, banks are also exposed to market risk, exchange rate risk, investment risk, exposure risk, legal risk, strategic, operational, and reputational risk (Lukić & Trišić, 2015; Agbata et al., 2917). These listed risks have been significantly relativized by the development of technology and business procedures. The trend in modern banking is the automation of all financial activities. Electronic payment systems solve most of the problems of the old, traditional payment method based on paper documents (Milošević, 2022). Nowadays, with the increasing development of new techniques and technologies, banks are more often facing losses resulting from fraudulent activities and misuse in the process of loan approval and card business (Čupović, 2023; Miladinović Bogavac, 2017). For this reason, in addition to the adequate assessment of credit risk, it is also important to manage the risk of fraudulent activities properly. Timely recognition of early indicators of fraud risk is essential in this process and contributes to the adequate management of credit risk by preventing potential fraudulent activities by users of banking services who are aware that they are

[1] Corresponding author: Tamara Đalić
Email: tamara.vesic@vspep.edu.rs

high-risk for banks (Đorđević & Đukić, 2015), or that they do not have a good credit score (suitable creditworthiness) and that, based on that, their credit requests will be rejected by banks where the requests are submitted. Adequate management of fraud risk directly affects the reduction of potential financial losses of banks (Vuković & Radović, 2014), and thus affects their ultimate business results.

## 2. Methodological framework and paper structure

The aim of this research is to assess the effectiveness of existing systems and practices for managing the risks of fraud in the banking sector of the Republic of Serbia. It involves providing information that has been collected and processed from real sources (Vesić et al., 2023). Presenting all the findings and certain solutions should contribute to preventing future credit and card fraud in banks and positively influence decision-makers at both the operational and top management levels.

The research in this paper explores the impact of potential fraudulent activities on the credit and card processes, as well as the overall risk management that potential fraudulent activities may cause in the banking system in the period before, during, and after the Covid-19 virus-induced pandemic, i.e., in the period from 2018 to 2022. The parameters of a real bank operating in the Republic of Serbia were observed within the research, but its business name will not be disclosed due to data sensitivity. Based on the above, the basic hypothesis of the paper is formulated as

**H0**: *Timely identification of indicators of fraud risk significantly contributes to adequate risk management in general.* It is further developed with auxiliary hypotheses:
**H1:** *The increase in credit fraud has an extremely negative impact on the success in managing credit risk.*

**H2**: *The most common methods of committing credit fraud are document forgery.*

**H3:** *Unsecured loans are more susceptible to fraudulent activities than secured loans*.

The scientific justification for the research is reflected in the application of scientific methods in the analysis of fraudulent activities in the banking sector, and the social justification for the research lies in the analysis of fraudulent activities and the finding of adequate ways to prevent, eliminate, or reduce them. The expected contribution is characterized by a description of recognized fraudulent activities in the observed bank, with the aim of establishing the characteristics of the profile of a potential perpetrator of fraudulent activities, and thus assisting mathematicians, analysts, managers, and bankers in preventing future potential losses of banks. Additionally, the research aims to demonstrate best practices in discovering the methods used by potential perpetrators of fraudulent activities in practice.

The paper is divided into appropriate sections to comprehensively analyze the complexity of managing the risk of fraudulent activities in the banking sector, which are descriptively described.

The first part of the paper relates to an introduction to the topic, briefly presenting the subject and objectives of the research, hypotheses are set up in the second part. The third part of the paper presents the results by presenting examples of credit and card fraud detected in the portfolio of a specific bank operating in the Republic of Serbia. Their impact on risk management of the overall portfolio and the bank's business itself is discussed. Finally, based on the conducted analyses, a descriptive description of those characteristics that most closely correspond to the profile of a potential perpetrator of credit fraud is provided. After presenting all the results and facts, a conclusion is drawn, along with recommendations for future research.

## 3. Results and discussion

Fraud represents a deliberate act with the aim of exploiting the other party unfairly or wrongfully gaining property benefits in an unworthy manner (Cogoljević et al., 2019; Arežina et al., 2016). It involves the intentional and purposeful preparation of documents, facts, information, and situations to create conditions in which someone, based on misrepresented facts in deliberate circumstances, is induced to believe in a falsehood and, in accordance with it, acts and, as a result, suffers a loss or harm (Škarić Jovanović, 2008). The Association of Certified Fraud Examiners (ACFE, 2016) defines financial fraud as follows: “Financial fraud is the intentional, deliberate, false statement or omission of material facts or accounting data, which, when viewed in conjunction with other information as a whole, leads the reader to change or rearrange their assessment or decision” (Rezaee & Riley, 2010; Dimitrijević, 2015). Frauds can be of external nature when they represent malicious activities by third parties towards a specific institution, or of internal nature (Mitrić et al., 2012; Wolfe & Hermanson, 2004), which includes intentional activities and/or omissions by at least one person employed within that institution for personal gain (Stanišić, 2007; Charvát Janechová & Bednárik, 2023). Such forms of fraud can have significant material losses for the specific institution, damage its reputation, jeopardize its market standing, negatively affect customer loyalty, and even compliance with regulations (Vuković et al., 2021; Petković, 2010).

The main challenges that banks face include finding adequate solutions to prevent potential fraud (Pavlović, 2023). The reasons for this are manifold. Trends in fraudulent methods are constantly changing, techniques for executing fraud are improving (Perović et al., 2022), and the complexity of fraud is increasing, making it difficult to effectively monitor various innovative banking products and sales channels (online, internet and mobile banking, expanding ATM machines, POS devices). Furthermore, inadequate data integrity: the inability to integrate and validate data from numerous banking channels and other data sources implies that they are often incomplete and unreliable (Kovinić et al., 2022). Limited analytical capabilities, or restrictions in transaction analysis that do not allow transactions to be effectively analyzed to identify suspicious behavior patterns, make banks susceptible to organized crime and illegal practices (Nedeljković, 2022). Limited human resources are also one of the reasons - the ability to prioritize work and appropriate activities in specific fraud cases is crucial for resource optimization, but it is challenging to achieve without an adequate solution (Malik et al., 2022). Another reason is the frequent changes in regulatory requirements.

The paper continues with the results of detected and prevented fraudulent credit and card transactions.

### 3.1. Credit operations

When discussing fraud in the financial sector, there are already defined patterns of behavior by applicants and specific indicators that suggest that the applicant is a potential issue (Đekić et al., 2016; Đekić et al., 2022). However, with the increasing development of new technologies, the techniques used in fraudulent attempts are also increasing and changing (Radić, 2021). Every day, banks are increasingly exposed to new techniques that significantly differ from the techniques previously used and which have already been recognized by banks as potential frauds, and their patterns have already been included in indicators that bank employees can use to identify potentially problematic behavior (Lukić, 2021).

In Table 1, an overview of changes in the bank's portfolio over a 5-year period is provided.

**Table 1.** The number of confirmed credit fraud cases during the period 2018 - 2022 compared to the number of approved loans during the same period.

| | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| Number of Confirmed Frauds | 66 | 70 | 29 | 24 | 196 |
| Number of Loans Disbursed | 21,995 | 28,122 | 20,776 | 32,599 | 54,092 |
| Percentages | 0.30% | 0.25% | 0.14% | 0.07% | 0.36% |

What can be clearly seen from the table is an increased number of confirmed credit fraud cases in 2018 and 2019, while in 2020 and 2021, the bank records a significant decrease in these numbers. Furthermore, the table also shows a significant increase in detected fraud cases in 2022. The explanation for the number of confirmed fraud cases in 2018 lies in the fact that individual loan users found a way to use earmarked loans for purposes not defined in the loan agreements. Specific examples include loans for refinancing. Refinancing, or early repayment of loans, requires compliance with the agreed procedure and a certain period of time. Most banks operating in the Republic of Serbia had instructions for refinancing loans that involved transferring funds intended for refinancing to the current account of the loan user. In this situation, the loan user is required to inform the bank whose loan products are being refinanced that the funds have been deposited into the current account for refinancing, and to submit a request for early repayment of the loan products being refinanced so that the bank's employees can transfer the funds from their current account to the loan products that are to be fully repaid with that money. Otherwise, the money will remain in the loan user's current account until they submit a request for early repayment, i.e., a request for transferring the funds to the loan products to be repaid with that money.

A certain number of loan users realized that banks themselves could not transfer the money from their current accounts intended for refinancing to the loan products to be repaid with those funds, and that they could not complete the refinancing process stipulated in the contract on their own. The situation was exploited by certain loan users who realized that they could withdraw money from their current accounts in multiple iterations at ATMs or transfer money from their current accounts through e-banking (or m-banking) in partial transactions to accounts they held in other banks. This behavior of loan users falls into a form of credit fraud since the provisions of the loan agreement were violated, and the money was used for a completely different purpose than what was defined in the loan agreement (Đekić et al., 2022). The result of this behavior was that loan users became doubly indebted—in the new bank for the amount of the new obligations for approved and disbursed refinancing loans, and in the banks whose loan products were supposed to be repaid with the funds intended for refinancing. In such situations, loan users quickly fell behind on their loan installments since their monthly incomes could not cover the burden of double indebtedness. Specifically, their creditworthiness couldn't bear the total financial burden resulting from practically taking out new loans for the amount of the refinancing loans that weren't used for their intended purpose—they became over-indebted with additional obligations.

Furthermore, organized fraud can be defined as the joint participation of more than three individuals in the same fraudulent scheme or criminal group. During 2019, Bank “A” was exposed to fraud by an organized group of individuals who, based on false information and falsified employment documentation, were granted and disbursed a significant number of loans, resulting in significant financial losses for the bank. Following this case, a series of activities were initiated by the bank to raise awareness among its employees about the importance of managing fraud risks and the prevention phase. This resulted in a reduction in confirmed fraud cases in the bank's portfolio in the following years.

From Table 1, it can also be observed that in 2020, there was a drastic decrease in the number of detected cases of credit fraud, as well as a reduction in production volume, i.e., the number of approved loans. The decreases in all these areas in 2020 are a direct result of the pandemic caused by the Covid-19 virus. During the state of emergency in the Republic of Serbia, which lasted from March 15th to May 7th, 2020, banks, like many other institutions, faced new challenges, potential problems, and possible losses due to the impact of the pandemic on the country's economy and business environment. During this period, due to restricted movement and curfew, banks operated under modified (shorter) working hours, and far fewer people applied for credit products, which is evident in the graphical representation on Chart 1. The number of approved loans decreased from 28,122 to 20,776. The number of detected fraud cases in the portfolio also decreased from 70 to 29.

However, what is crucial for the operation of “A” bank in 2020 is the number of fraud cases that were detected before the bank approved loans and disbursed funds. This period is the best indicator that, with appropriate measures taken after the 2019 case and increased portfolio control, the bank successfully approached risk management for fraud. In the case of bank “A,” the focus in 2020 was entirely on prevention as the most critical phase in fraud risk management. Several new defense mechanisms were implemented both within the bank’s system and through employee training, which saw a significant increase in frequency compared to previous years. An approximate profile of individuals more likely to commit credit fraud was established, and detailed guidelines were provided to help bank employees identify potential fraudulent activities more easily, quickly, and efficiently.

These preventive activities resulted in 2021, with the highest number of prevented cases during the observed four years (a total of 586 cases), and the lowest number of detected credit fraud cases in the portfolio (24 cases). However, an interesting fact that can be seen in Table 1 and Graph 1 is the drastic change in the number of detected fraud cases in the bank's portfolio in 2022 compared to 2021, as well as compared to all previous years. In 2022, the bank experienced a significant increase in detected fraud cases of almost 8 times (196 confirmed credit fraud cases). What led to this sudden change? The introduction of a new product with which the bank had no previous experience. At the end of 2021, a new product was introduced - consumer loans for devices that only began to expand in the first half of 2022. These are short-term unsecured loans with maximum amounts that are small, up to EUR 750.

In the case of this type of credit, the bank enters into a contract with the borrower through an intermediary (partner merchant). These consumer loans are approved based on the borrower's ID card without the need for additional documentation, such as employment confirmation and income level, and without collateral (administrative bans or promissory notes do not exist in the process). Since it was a completely new product for bank “A” with no previous experience, the controls and rules established in this process were insufficient to prevent a large number of individuals from taking out loans based on false information during 2022. Thus, in 2022, most credit fraud cases were based on granting loans to individuals who provided false information about their employment through the merchant partner. In each of these fraud cases that were detected, it turned out that these individuals had never worked for the employers they claimed when applying for the loan. Out of a total of 196 confirmed fraud cases that occurred at bank “A” in 2022, a staggering

186 cases were related to this fraudulent scheme (Figure 1), highlighting the importance of collateral and well-established controls in preventing fraudulent activities.

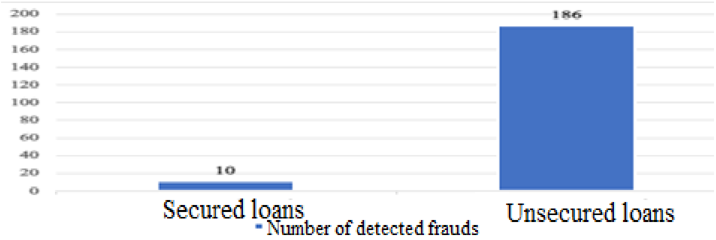

**Figure 1.** Graphic representation of the number of confirmed credit fraud cases in relation to the type of secured and unsecured loans

In addition to credit risk, effective management of the risk of fraudulent activities also contributes to a certain extent to the reduction of NPLs in banks. NPLs represent loans that have been declared due, meaning loans that have matured or have not been repaid in accordance with the agreed repayment terms (Beslać, 2019; Barjaktarović et al., 2021). NPLs can be defined as problematic loans for banks. The concept of problematic loans involves loans where there are issues with repayment for one or more reasons. A loan can be classified as non-performing from the moment when neither any portion of its principal nor interest has been collected for the last 90 days, according to the terms defined in the loan agreement when it was granted. Figure 2 provides a representation of the share of confirmed credit fraud cases in the total NPL amount of Bank “A” in March 2022. The total NPL in March 2022 amounted to 1,655,000 EUR, of which 178,302 EUR was related to loans for which it was confirmed that they involved credit fraud. Percentage-wise, the proportion of loans with detected fraud indicators and confirmed fraud cases in March 2022 was 0.108% of the total NPL amount.

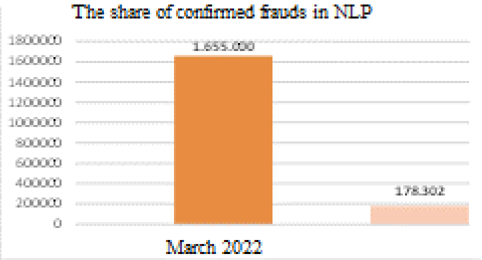

**Figure 2.** The share of confirmed credit fraud cases in the total NPL for the month of March 2022 for Bank “A”

### 3.2. Credit operations

When we talk about the risk related to transaction payments and credit cards in the modern environment, physical misuse of credit cards (such as physical theft of credit cards) is decreasing, while abuses through the internet or special devices for stealing credit card data are increasing. On one hand, mechanisms are rapidly developing to make card transactions more secure. However, on the other hand, with the parallel development of new techniques and technologies and increased use of online banking services, online shopping, and internet payments, the number of fraud attempts and credit card misuse is also on the rise (Stakić & Stefanović, 2023).

The pandemic caused by the Covid-19 virus has further contributed to the shift from traditional physical credit card fraud to more modern and complex methods of theft, especially online and contactless, which are harder to detect. Preventing such fraud requires substantial financial investments and increased efforts to find new defensive mechanisms by banking institutions. The same phases of the fraud prevention cycle are recognized in card transactions and potential fraudulent activities that may occur during the use of credit cards (Radović Marković et al., 2022). The majority of frauds are usually discovered through employee reporting, and for this reason, employees are considered the first line of defense against embezzlement, theft, and malfeasance.

When discussing fraud in card transactions, it primarily refers to the misuse of credit cards that can occur. Fraud in card transactions generally begins with the physical theft of the card itself or compromising the personal data associated with the card, including the current account number or any other information available to the payee during a transaction or payment for a specific purchase. With credit card misuse, there is also the possibility of identity theft for the cardholder.

In situations where a credit card is physically stolen or lost by the cardholder, it remains in use until the cardholder notifies the bank of its loss. The thief who has stolen the credit card may use it for unauthorized purchases and payments until the cardholder reports its disappearance and the bank, which issued the credit card, blocks the cardholder's account associated with the stolen card. Information about the account linked to the credit card is stored in various formats. The credit card itself contains basic cardholder information, including the name, surname, and signature. Additionally, the card also features the account number, a magnetic stripe with machine-readable data, and a CVV or CVC number. This CVV or CVC number serves as a security code used for additional user authentication, primarily for validating card-not-present payments, such as those made over the internet when the physical card is not present.

Identity theft, in addition to stealing money from a cardholder's account, involves the theft of the cardholder's personal data. This type of fraud is typically carried out online through various manipulations and fraudulent activities by those seeking unauthorized access to all of the cardholder's information. In cases of identity theft, the perpetrator of the fraudulent activity uses the cardholder's data to make purchases, conduct other payment transactions, and even open accounts in other banks in the cardholder's name. In recent years, fraud in this manner often involves the thief depositing a minimal amount into the real cardholder's account to avoid drawing attention from the bank, as they have met the minimum monthly payment requirements. Nevertheless, the cardholder's account becomes increasingly indebted each month, and when the cardholder notices that money is missing from their account, it can be challenging to prove that they did not carry out those transactions themselves and that the missing funds are a result of credit card and account misuse.

Data skimming refers to the theft of data from payment cards used in legitimate transactions. Perpetrators of this type of fraud can obtain a card's information by copying receipts or using more advanced methods such as small electronic devices designed to copy card data when they come into close proximity to the card.

Data theft, known as skimming, involves stealing the magnetic stripe data from an original payment card using a small device called a skimmer. These small electronic devices are typically compact, about the size of a matchbox, and are often placed on ATMs – either on the ATM's keypad, camera, or at the card entry slot. When a person tries to withdraw money or insert their card into the ATM, the skimmer can even capture the user's PIN code. Such devices are invisible to the naked eye as they are practically seamless with the ATM. Therefore, the user is often unaware that someone unauthorized is accessing their data and stealing it while using the ATM. The skimmer optically reads and collects data from the magnetic stripe on the original payment card. All the user's data obtained in this way is wirelessly transmitted to the perpetrator of the fraudulent activity. What characterizes this type of data theft is that the attempts are more common over weekends because it's harder to report such incidents to banks due to their limited working hours during these days.

Phishing is a cheap and simple method for unauthorized data collection regarding payment cards and their users. Phishing is an online scam that usually happens through emails sent by the fraudster to steal cardholder data. This type of attack represents the most harmful form of fraud. The majority of these attacks come through email messages that typically claim there's an issue with the user's account and kindly ask them to provide their details to resolve the problem. Sometimes the perpetrator of such fraudulent activities includes a link in the email leading to a website that appears nearly identical to the user's regular platform for transactions.

Another form of this type of fraud is known as Vishing, which is a newer form of phishing that involves data collection through a conversation over a phone call. It's essential to note that a perpetrator of fraud doesn't have to physically obtain a payment card to withdraw money from an account. Common methods include scanning and copying the card's data, as well as hacking the user's online account. Perpetrators of fraudulent activities can easily obtain cardholder data, which typically includes the card number, expiration date, and the three-digit security code on the back of the card (CVV code), used for online transactions and payment confirmation. This data can be most easily acquired by photographing or scanning the payment card. It can happen that someone photographs the user's payment card while they're waiting in line to pay at a checkout. If the user accidentally leaves their wallet or card in their hotel room, it's also possible for someone to take a picture of it.

One of the most significant trends in banking today is digital transformation. Technology has always had an impact on the banking sector and its operations. However, the current phase is dramatically different in terms of the scope and pace of change. The combination of technology and digital has the potential to change everything. This combination can provide access to new products and services and change the way certain business activities are traditionally conducted.

With this kind of rapid, dynamic change that requires constant innovation and creative solutions, especially in online activities, there's more room for the advancement of potential fraudulent schemes in all aspects of business, particularly in the banking sector.

**Table 2.** The number of cases of prevented and confirmed credit card fraud in the period 2018 - 2022

| | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| The number of issued cards | 1,884 | 2,997 | 3,830 | 7,648 | 11,095 |
| The number of prevented fraud attempts | 24 | 56 | 433 | 1.065 | 2.260 |
| The number of confirmed frauds | 0 | 0 | 37 | 64 | 100 |

Table 2 provides an overview of the number of prevented fraud attempts and cases where there was reasonable suspicion of fraudulent activity that Bank “A” faced during the observed period. Additionally, from the same table, you can see how the total number of issued payment cards changed over the 5-year period. This number showed an upward trend, increasing each year, with the number of issued cards in 2022 being almost six times higher than in 2018.

Furthermore, it is evident that the interest in payment cards increased during the COVID-19 pandemic and continued to grow even after the pandemic. The reason for this lies in the development of electronic commerce and the significant rise in online shopping, which was facilitated by the pandemic and the lockdown measures in 2020. During the lockdown, people shifted their focus to online shopping. This trend persisted post-pandemic as individuals realized that using payment cards could greatly simplify and expedite the shopping and payment process.

However, it is also noted that there was an increase in fraudulent activities that corresponded with the growth in the number of issued cards. The number of fraud cases rises alongside the increase in the number of cards in use. As users of payment cards embraced the convenience of daily life through increased card usage, fraudsters also found new ways to exploit cards and engage in various forms of theft.

With the expansion of online shopping, the number of malpractices and payment card abuses over the internet has also increased.

**Table 3.** The number of suspicious transactions and declined transactions due to confirmed fraud in relation to the total number of transactions in 2021 by quarters.

| | Q1 2021 | Q2 2021 | Q3 2021 | Q4 2021 |
|---|---|---|---|---|
| Total number of transactions | 960,242 | 1,418,541 | 1,588,560 | 1,725,786 |
| Suspicious transactions | 3,506 | 5,858 | 7.678 | 9,309 |
| Declined transactions | 1,637 | 1,678 | 1,533 | 1,999 |

Table No. 3 provides data on the total transactions that occurred during 2021. The data is presented by quarters to highlight changes in the transaction structure, showing how the number of transactions significantly increased from quarter to quarter. In just one year, an incredible change is observed. The difference in the number of transactions at the beginning and end of 2021 is substantial. In the last quarter, the number of transactions increased by almost 100%, meaning that the number of transactions at the end of 2021 doubled compared to the number at the beginning of the year. However, as mentioned earlier, with the increase in the total number of transactions, the number of suspicious transactions also rises, consequently leading to more transactions being confirmed as attempted fraud. Table No. 3 contains data on prevented fraud attempts and misuse of payment cards, i.e., transactions whose execution was rejected due to well-founded suspicion of fraudulent activity.

Tables 3 and 4 confirm the rapid development of card transactions and the increasing use of payment cards from month to month. They also illustrate the growing number of attempted fraudulent activities.

The Table 4 provides data for the year 2022, also broken down by quarters to offer a detailed overview of changes in the bank's card portfolio.

The trend of increasing the total number of transactions from 2021 carried over into 2022, and the difference in the growth of that number can be seen from quarter to quarter.

**Table 4.** The number of suspicious transactions and rejected transactions due to confirmed frauds in relation to the total number of transactions in 2022 by quarters

| Period | Q1 2022 | Q2 2022 | Q3 2022 | Q4 2022 |
|---|---|---|---|---|
| Total number of transactions | 1,675,248 | 1,710,613 | 1,897,134 | 1,973,546 |
| Suspicious transactions | 6,959 | 5,787 | 9,331 | 12,794 |
| Declined transactions | 1,121 | 1,781 | 4,003 | 3,275 |

Additionally, there is continued growth in transactions that are considered suspicious, as well as transactions that are rejected due to confirmed frauds. When it comes to confirmed frauds and abuses in Bank A's card business, online fraud with transactions takes the top spot, meaning abuses of payment cards via the internet. These abuses are executed in one of the following two ways. The first method is known as BIN attacks. These attacks occur when the perpetrator activates specific software that initiates thousands of transactions until one of those transactions “hits.” These are software attacks that work based on mass random attempts within seconds. When they “hit” the card number, CVV code, and card expiration date, they continue to execute transactions with the same combination, from larger to smaller amounts, as long as these transactions are approved. The BIN (Bank Identification Number) is found on the payment card. The card number is called PAN, which can have from 13 to 19 digits, with the most common being 16 digits, grouped into 4 sets of 4 digits. Often, the first 6, or recently the first 8 digits of the PAN, are referred to as the BIN. Starting from a few years ago, when we talk about BIN, we may also encounter the term IIN because card issuers are no longer just banks; they can be other payment institutions. In this case, banks and products that do not have a good protection system and tools capable of recognizing such mass attacks are targeted by fraudsters. Banks defend themselves against this type of attack with certain “smart” tools that operate based on artificial intelligence (AI) and are capable of learning from large databases. These tools, based on statistics, automatically approve or reject transaction execution attempts. The second method involves the classic theft of data over the internet, through certain websites designed exclusively for abusing payment cards. A user of a payment card, who makes a purchase through such an unreliable website, by entering personal information and card data, provides the perpetrator of fraud with the opportunity to acquire the user's information in an unauthorized way and use it further for stealing money from their current account or for unauthorized transaction execution.

As the second method of committing identity theft of payment card users, phishing often appears. In most cases of phishing, the user's email is abused to make the user send their personal information directly to the perpetrator of the fraud. Alternatively, an email is sent to the user with a link to a website where the user is supposed to access and provide their personal information and card details. Social networks are also frequently used for conducting phishing attacks. The principle is the same as when emails are sent by the perpetrator. In the user's inbox through a certain social network, a message arrives in which the perpetrator asks for the user's personal data, with a specific explanation of the purpose for which this information is needed. In such situations, scanned or photographed images of the payment card (both sides of the card) are often requested, or a link is sent through which the user of the payment card is required to access a specific website and enter their information and card details. Malpractices conducted in this way often result in multiple transactions from the user’s account in smaller amounts.

Somewhat less common methods of attempting to abuse payment cards in recent years include data theft via skimming and card counterfeiting (creating fake cards). However, these more traditional methods of credit card fraud, while occurring to a lesser extent in modern environments, still exist and are present in the market.

At the bottom of the list of payment card abuses are physical thefts of payment cards, meaning the physical theft of the original card (plastic). In today's world, with the advent of contactless payment cards, perpetrators of physical card theft can use the card for purchases or payments up to the amount allowed by contactless payments (usually around 5,000 RSD in the Republic of Serbia). However, banks typically send an SMS notification to the cardholder after the transaction has been completed and money has been withdrawn from the checking account, informing the cardholder of the location, time, and amount of the transaction. This allows the cardholder to quickly report the theft to the bank and prevent further misuse. For this reason, physical card theft has become a less attractive method of abuse for perpetrators in recent times.

## 4. Establishing the profile of a fraud perpetrator

It is essential to ask whether some individuals are more likely to commit fraudulent acts than others. Typically, it is assumed that various external factors motivate and drive people to commit fraud, such as economic conditions, socio-political factors, competitive factors, poor internal control mechanisms, etc. (Vona, 2008). In addition to external factors, it is crucial to recognize personality traits and internal motivators of those attempting fraud. It is clear that it is not possible to create a perfectly accurate profile of a potential fraudster that could be used for precise fraud detection. Identifying indicators of fraudulent activity often requires months, even years of learning, experience, and working to understand and recognize certain signals that suggest potential fraud. However, to get as close as possible to an accurate answer to the question you posed, specific analyses have been conducted on Bank “A”’s portfolio. The results of these analyses, which will provide insight into who is more inclined to commit fraudulent acts, are presented in this paper.

Table 5 illustrates the relationship between the education level of users with identified risk indicators, specifically those who have been confirmed to commit credit fraud and have received a loan from “A” Bank based on false and inaccurate information. The analysis covers a two-year period, 2020 and 2021. From Table 5, it can be concluded that the largest number of fraudulent actions aimed at obtaining loans was committed by individuals with a secondary education level, i.e., those who have completed high school.

**Table 5.** The relationship between the level of education and the number of confirmed credit card frauds in the period 2020-2022

| Level of education | Primary education | Secondary education | College/University | Master’s | No education data |
|---|---|---|---|---|---|
| Number of Confirmed Frauds in: | | | | | |
| 2020 | 0 | 20 | 4 | 0 | 5 |
| 2021 | 0 | 16 | 7 | 0 | 1 |
| 2022 | 15 | 151 | 30 | 0 | 0 |
| Total | 15 | 187 | 41 | 0 | 6 |

According to data from "A" Bank, Table 6 shows that the number of individuals to whom loans were fraudulently approved and disbursed in "A" Bank is concentrated around the age group of 31 to 40 years in 2020. However, in 2021, there is an increase in credit fraud committed by individuals younger than 30 years. This can be attributed to the consequences of the Covid-19 pandemic, the restrictive policies of banks towards individuals with no credit history, the development of new techniques and technologies that are more accessible to younger populations than older ones, and the fact that younger individuals often require more additional funds, which can be "easily" earned.

**Table 6.** The number of detected credit frauds relative to the ages of individuals who committed fraud.

| Age Categories of Individuals | up to 30 | 31-40 | 41-50 | 51-60 | over 60 |
|---|---|---|---|---|---|
| Number of Detected Credit Frauds in: | | | | | |
| 2020 | 10 | 2 | 9 | 7 | 1 |
| 2021 | 9 | 7 | 1 | 5 | 2 |
| 2022 | 79 | 47 | 34 | 25 | 11 |
| Total | 98 | 56 | 44 | 37 | 14 |

Table 7 shows the impact of the average income on the total number of detected frauds in the portfolio of bank "A." What can be concluded from the data presented in Table 7 is that a significant number of credit frauds were recorded during 2020, committed by individuals with average monthly incomes ranging from RSD 40,001 to RSD 50,000. The situation is somewhat different in 2021 when the bank "A" portfolio witnessed an increase in the number of frauds committed by individuals with average earnings in the range of RSD 30,001 to RSD 40,000.

**Table 7.** The influence of the average income level on the total number of confirmed credit frauds in the period from 2020 to 2022

| Average income (RSD) | up to 30,000 | 30,001-40,000 | 40,001-50,000 | 50,001-60,000 | over 60,001 |
|---|---|---|---|---|---|
| Number of Confirmed Frauds in | | | | | |
| 2020 | 5 | 5 | 11 | 3 | 5 |
| 2021 | 1 | 8 | 3 | 3 | 9 |
| 2022 | 0 | 18 | 35 | 63 | 80 |
| Total | 6 | 31 | 49 | 69 | 94 |

Gender is also a factor that can contribute to profiling individuals who are willing to commit fraudulent acts. Earlier in the paper, there was mention of research conducted by the auditing firm KPMG (KPMG, 2011) based on 348 active cases of financial fraud in 69 countries. Among the results of this research, one of the findings was that the perpetrators of fraudulent acts were predominantly male. The analysis results from KPMG's research are corroborated by the analysis of cases of credit fraud detected in the portfolio of "A" bank. During the period 2020-20212 the total number of detected loans approved through fraudulent actions amounted to 249 credit applications.

Out of these 249 individuals, a significant 141 were males (57%).

Based on all the analyses conducted on the portfolio of “A” bank and the obtained results, the following conclusions can be drawn: The majority of credit frauds were committed by male individuals under the age of 40 with a moderate level of education and average monthly income ranging from RSD 30,000 to RSD 50,000. It is essential to note that risk indicators for fraudulent activities almost never occur individually. They typically appear in combination with multiple different indicators, multiple signals that, when detected and recognized in time, can contribute to a quicker response to prevent individuals from committing the intended fraudulent activity.

## 5. Conclusion

The modern business environment, shaped by globalization, the increasing use of advanced technologies and innovations in business, as well as the consequences of the global economic crisis, growing competition, and demanding clients, is characterized by a rising number of frauds that are becoming increasingly complex and have lasting effects on banks’operations. As a part of credit risk, in the modern era, with the emergence of new techniques and technologies, banks are exposed to more frequent attempts at financial frauds because the activities carried out by these banks as financial institutions enable wrongdoers to gain direct financial benefits with minimal investments. Committing fraud inflicts damage on banks both materially and reputationally. Many banks find it difficult or impossible to recover from the consequences that certain fraud cases can cause – their reputation is permanently tarnished, and in an environment where cost minimization is often a competitive advantage, financial losses, often measured in hundreds of thousands of euros, are frequently insurmountable obstacles for the continued existence of banks. Therefore, banks are increasingly focusing on developing and implementing various mechanisms to combat fraud.

With the accelerated development of various techniques and technologies worldwide, as well as in Serbia, different forms of fraud and malpractice are emerging. The misuse of payment cards represents only a part of fraudulent activities that can be identified in the banking sector and business. The primary challenge for banks in such fraudulent activities is finding ways to protect the user from the misuse of payment cards. Banks and other financial institutions strive to keep up with this by attempting to adequately protect their clients through the development of new security mechanisms, improving ATMs, and introducing new types of cards aimed at increasing user security.

In this paper, using the example of Bank “A,” based on the number of detected credit frauds in the Bank “A” portfolio, H0 has been proven, demonstrating that adequate credit risk management, accurate assessment of credit requests, and the timely identification of indicators for fraudulent activities play a crucial role in the fight against fraudulent actions in the banking sector. Recognizing early signals indicating that a particular individual is likely to commit a fraudulent action allows the bank to prevent potential fraud in a timely manner, thereby preventing potential losses that could result from the execution of fraud. During the analysis of Bank “A’s” portfolio, H1 demonstrated a noticeable negative impact of credit fraud on credit risk management. The increase in unprevented fraudulent activities negatively affects the bank's operations, potentially causing losses in the future. The rising number of confirmed credit frauds negatively affects the bank's portfolio, contributing to the increase in problematic loans or the rise of NPLs.

H2 - The most common type of fraud resorted to during the Covid-19 pandemic was fraud based on forged documentation. In the observed period, Bank "A" faced a significant credit fraud carried out using falsified documentation in 2019. The trend of attempts with the same pattern continued the following year, but with the application of lessons learned from 2019 and adequate measures, attempts at credit fraud were brought under control in 2020. Bank "A" suffered a higher number of fraudulent "attacks" in 2022. This year also emphasizes the importance of properly managing credit risk. During the introduction of a new product into Bank "A's" portfolio in this year, the bank failed to assess the credit risk correctly and did not establish adequate controls, which automatically resulted in an increased number of detected fraudulent activities in 2022.

Statistical data from 2022 confirm H3 – that individuals applying for unsecured loans are more susceptible to fraudulent activities, i.e., the number of credit frauds with unsecured loans is far greater than that with loans where collateral exists. In the case of unsecured loans, perpetrators of fraudulent activities are driven by the fact that if there is no collateral for the loan (not even minimal, such as an administrative order or promissory note), in case of default, the bank will not be able to find a way to collect the outstanding debt from them. For this reason, with unsecured loans, a larger number of individuals are more inclined to provide false information when submitting a credit application compared to loans that have collateral.

The paper also provides a profile of a potential fraudster, contributing not only to the academic but also to the professional community. As a result of the research, a potential fraudster is a male, with a medium level of education, between 30 and 40 years of age, and an income exceeding 60,000.00 RSD.

What will undoubtedly be a challenge for banks in the future are further changes in the methods of conducting credit frauds, their further modification, and the refinement of techniques used by individuals willing to commit fraudulent actions, on one hand, and finding the best solutions to recognize and prevent attempted frauds in a timely manner, on the other. Banks are increasingly shifting their operations to the Internet, improving electronic banking. This way, in the future, banks will be more exposed to cyber frauds. However, what is equally certain is that attempts at traditional fraud will remain present in their business.

## References

ACFE. (2016). Report to the Nations on Occupational Fraud and Abuse. *Fraud Magazine*, 4-85.

Agbata, A. E., Ekwueme, C. M., & Jeroh, E. (2017). Anatomija prevara u penzionim fondovima u Nigeriji - njihovi motivi, upravljanje i budućnost

sistema penzionog osiguranja u Nigeriji. *Ekonomski horizonti*, *19*(3), 179-191. https://doi.org/10.5937/ekonhor1703179A

Arežina, N., Mizdraković, V., & Knežević, G. (2016). Profesionalne prevare kao pretnja funkcionisanju privrednih društava. *FINIZ 20166* (str. 209-213). Beograd: Univerzitet Singidunum. doi:DOI: 10.15308/fi niz-2016-209-213

Barjaktarović, L., Vesić, T., Laki, B. (2022). What can be Eexpected in Credit-Risk Management from NPL in the Western Balkans Region in the Future*? International Review*, (3-4), 96-103.

Beslać, M. (2019). *Korporativne finansije*. Beograd: Visoka škola za poslovnu ekonomiju i preduzetništvo.

Charvát Janechová, J., & Bednárik, J. (2023). Uticaj korporativnog identiteta na reputaciju i brend poslodavca. *Serbian Journal of Management*, *18*(1), 59-69. https://doi.org/10.5937/sjm18-37903

Čupović, S. (2023). Kamata u Kur'anu i njene posljedice na savremeni svijet. *Ekonomski izazovi,* 12(23), 101-111. https://doi.org/10.5937/EkoIzazov2323101C

Đekić, M., Filipović, P., & Gavrilović, M. (2016). Forenzičko računovodstvo i finansijske prevare u svetu. *Ekonomija: Teorija i praksa, 9*(4), 71-86.

Đekić, M., Nikolić, M., & Vesić, T. (2022). Nastanak i trendovi razvoja elektronskog bankarstva u Srbiji. *Trendovi u poslovanju, 10*(1), 97-108. https://doi.org/10.5937/trendpos2201101D

Dimitrijević, D. (2015). Otkrivanje i sprečavanje manipulacija u bilansu stanja i izveštaju o novčanim tokovima. *Ekonomski horizonti*, *17*(2), 137-153. https://doi.org/10.5937/ekonhor1502137d

Đorđević, M., & Đukić, T. (2015). Doprinos interne revizije u borbi protiv prevara. *Facta universitatis - series: Economics and Organization, 12*(4), 297-309.

Đukić, Đ. (2003). Bankarstvo. Beograd: Ekonomski fakultet.

Gogić, N. (2022). Prevare u finansijskim izveštajima. *Oditor, 8*(1), 7-35. https://doi.org/10.5937/Oditor2201007G

International, KPMG. (2011, 06 01). Analysis of Global Patterns of Fraud. Preuzeto sa https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

Knežević, S., Živković, A., & Milojević, S. (2021). Uloga i značaj interne kontrole i interne revizije u sprečavanju i identifikovanju prevarnih radnji u bankama. *Bankarstvo, 50*(1), 66-89. https://doi.org/10.5937/bankarstvo2101066K

Kovinić, N., Savić, M., & Pavlović, N. (2022). Analiza e-bankinga u vremenu korone. *Ekonomski signali: poslovni magazin*, *17*(2), 169-183. https://doi.org/10.5937/ekonsig2202169K

Lukić, L., & Trišić, M. (2015). Upravljanje rizicima i prinosima u bankama. *Trendovi u poslovanju, 3*(1), 28-39.

Lukić, R. (2021). Analiza efikasnosti finansijskih institucija u Srbiji na bazi OCRA metode. *Tehnika, 76*(1), 103-111.

Malik, G., Singh, D., & Stakić, N. (2022). Razumevanje bihevioralne namere o usvajanju Internet bankarstva - indijska perspektiva. *The European Journal of Applied Economics*, *19*(1), 110-120. https://doi.org/10.5937/EJAE19-35277

Miladinović Bogavac, Ž. (2017). Poslovne prevare u sajber prostoru. *Ekonomika, 63*(4), 97-104. https://doi.org/10.5937/ekonomika1704097M

Milojević, N. M. (2016). Savremeni izazovi u upravljanju rizicima banaka. *Poslovna ekonomija,* 10, 66-85.

Milošević, Đ. M. (2022). Frekventni oblici ispoljavanja internet prevara. *Baština, 56*, 209-227. https://doi.org/10.5937/bastina32-35814

Mitrić, M., Stanković, A., & Lakićević, A. (2012). Forenzičko računovodstvo - karika koja nedostaje u obrazovanju i praksi. *Management - časopis za teoriju i praksu menadžmenta, 17*(65), 41-50.

Nedeljković, I. (2022). Determinante i konsekvence poverenja korisnika mobilnog bankarstva. *Bankarstvo, 51*(3-4), 170-201. https://doi.org/10.5937/bankarstvo2204170N

Pavlović, G. (2023). Efekti pandemije COVID-19 na ljudski kapital i finansijske performanse - slučaj bankarskog sektora Srbije. *Anali Ekonomskog fakulteta u Subotici*. Advance online publication. https://doi.org/10.5937/AnEkSub2300022P

Perović, N., Abramović, N., Vukčević, N., & Ristanović, B. (2022). Analiza primene elektronskog bankarstva u Crnoj Gori u doba pandemije. *Ekonomski pogledi*, *24*(1), 279-301. https://doi.org/10.5937/ep24-38917

Radović Marković, M., Vesić, T., & Đekić, M. (2022). Monetary and financial cash flows as drivers of foreign direct investments at the global level. *International Review, 1-2*, 10-16. https://doi.org/10.5937/intrev2202013R

Stakić, N., Stefanović, N. (2023). Unlocking the Potential: Exploring the Impact of ETF Investments on the Global Fintech Landscape. *International Journal for Quality Research 17*(3), 963-974.

Stanišić, M. (2007). *Uloga interne revizije u otkrivanju i sprečavanja prevara u bankama*. Retrieved on 06 11, 2022 from UBS-Bankarstvo: https://www.ubs-asb.com/Portals/0/Casopis/2007/1_2/UBS-Bankarstvo-1-2-2007-Stanisic.pdf

Vesić, T., Gavrilović, M., & Petronijević, J. (2019). The influence of liquidity and profitability on the banking sector performances: The example of Serbia. *International Review* (1-2), 75-81.

Vesić, T., Gavrilović, M., & Vesić, J. The Assessment Revision of the Mechanisms Efficiency in Risk Management in the Serbian Banking Sector – Focusing on External Fraud. Conference Proceeding from 12th International Scientific Conference EEE2023 – in publishing

Vona, L. (2008). *Fraud risk assessment: Building a fraud audit program*. New Jersey: Wiley and Sons.

Vuković, I., & Radović, M. (2014). Pravno-političko opravdanje krivičnog dela korišćenja platnih kartica bez pokrića. *Anali Pravnog fakulteta u Beogradu,* 62(2), 68-85. https://doi.org/10.5937/AnaliPFB1402068V

Vuković, M. V., Vuković, A. A., Mladenović Ranisavljević, I. I., & Urošević, S. M. (2021). Analiza odnosa između korporativnog identiteta, imidža i reputacije preduzeća. *Tehnika*, *76*(4), 499-505. https://doi.org/10.5937/tehnika2104499V

Wolfe, D., & Hermanson, D. (2004). The Fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 38-42.

**Nikola Stefanović**
Faculty of Business in
Belgrade,
Singidunum University,
Belgrade, Serbia
nstefanovic@singidunum.ac.rs
ORCID 0000-0003-4554-7547

**Tamara Đalić**
Faculty of Business Economics
and Entrepreneurship,
Belgrade, Serbia
tamara.vesic@vspep.edu.rs
ORCID 0000-0002-5747-7542

**Jovana Vesić**
Faculty of Business Economics and
Entrepreneurship
Belgrade, Serbia
jovanavesic7@gmail.com