SOCIETY. INTEGRATION. EDUCATION
Proceedings of the International Scientific Conference. Volume II, May 26th, 2023. 467-477

CONTACTLESS PAYMENTS FRAUD DETECTION METHODS AND IS SOCIETY PREPARED TO RESIST: A CASE STUDY

Jelena Mamčenko
Vilnius College of Technologies and Design, Lithuania

Brigita Šustickienė
Vilnius College of Technologies and Design, Lithuania

Jūratė Romeikienė
Vilnius College of Technologies and Design, Lithuania

Abstract. *The ability to use contactless payment technologies, non-cash payments and credit card payments is becoming almost an essential requirement for consumers and merchants in today's economic conditions. Different market sectors are rapidly adapting to these technologies and looking for the most convenient, secure, and fastest possible solutions that combine intelligent data processing, security, and business management functions. Millions of debit and credit card holders care about secure payments, the businesses that receive these payments are secure in terms of security, and the operators that process such incoming and outgoing payments are interested in innovative solutions that set them apart from the competition. Amid the COVID-19 pandemic, when e-commerce was growing exponentially, the global market for fraud detection and prevention, currently stands at USD 20.9 billion, and is expected to grow, until 2025 will rise to USD 38.2 billion by the end of the year; holds the market at 12.8 % annually. The US remains the dominant region in this market segment, but European countries are also increasingly investing in fraud prevention and detection solutions, which are growing in demand in Europe due to an increase in cybercrime as well as advanced bots and cyber-attack.*
Keywords*: credit cards, contactless payment, data mining, fraud, unsupervised learning*.

Introduction

The use of plastic cards has now become a part of our daily lives, most have appreciated the convenience of this banking service. You do not need to carry a large amount of money with you, while this money can be used at your discretion at any time, both for purchases and payment of services, as well as for transfers to loved ones and friends . Recently, however, more and more people have fallen victim to credit and debit card fraud.

https://doi.org/10.17770/sie2023vol2.7159

According to the Nilson Report, which includes the card and mobile payments industries, the global card fraud losses amounted to $31.6 billion in 2018 and increased to $32.82 billion in 2019. In 2018, the European Central Bank reported that the value of fraudulent transactions accounted for about 0.04% of the total amount. This report and many others confirm the importance of early detection of fraudulent credit card transactions. However, current payment fraud detection algorithms mainly target merchants, fraud prevention algorithms that meet banking and FinTech security standards, and anti-fraud algorithms cheat. Intelligence-based fraud is few in number and functionally limited.

Other smart payment methods include contactless payment via phone or with phone stickers, smart watch contactless payment, payment ring, payment smart bracelet. Credit card purchase limit, biometric authenticated, phone contactless payments available for smartphones only.

Contactless payments continue to grow in popularity: according to the Lithuanian Bankers Association (LBA), in the first quarter of 2021, almost 70% of card payments in stores are made contactless, and approx. 10% is done by smart device.

In 2020, in Lithuania, the rate of contactless payments among customers with bank cards was 54% compared to other Baltic countries, while in Latvia, the rate of contactless payments were about 58% in total card payments. In Estonia, contactless payments were used once out of every four when paying by card, which is 27 cases in all payments.

The digital technology market has grown significantly during the COVID-19 pandemic and continues to grow. According to various studies, more than 60-70% of users are currently using one or more digital platforms, for example: transact online through your bank's mobile app, use digital wallet features, and more. These payment features allow the market to not be closed during the global quarantine. On the other hand, the need to ensure payment and prevent payment fraud cards is increasing. The ability of a payment processor to integrate advanced technology solutions (artificial intelligence, big data management, machine learning, deep learning, behavioral analytics algorithms, etc.). The accounting and tools used by the user bank are key factors in fraud detection. However, there is no proven and reliable single prevention tool yet.

One of the main tasks of the article is to find out how much people are familiar with possible cases of credit card fraud, whether they are ready to resist and not fall into the fraudsters' trap.

Literature Review

Credit card fraud is a form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it (An official website of the United States government, 2021; Cornell Law School, 2023).

This can happen by using one of your existing bank or online service accounts, via theft your physical bank card or your account numbers and PINs, or by opening new card accounts in your name without your permission.

The Bank (cardholder) is well aware of this and is constantly developing new measures to prevent unauthorized card usage. At the same time, however, clever fraudsters (including international organized crime syndicates) are always on the lookout for new security tools.

According to E. Starbuck Gerson (2023) there are three types of credit card fraud:

Card Theft: This is an old-fashioned way of stealing a physical credit card, either from a restaurant table or from an entire wallet or purse. Some criminals try to steal newly issued cards from mailboxes. If your card is lost or you receive notification that you were due to receive a card that never arrived, notify the issuer immediately. Account Takeover: An attacker contacts your card issuer and uses your personal information to change your login PINs, passwords, mailing addresses, etc. so they can take control of your account (and lock you out). Depending on how often you use your account, it may take some time for the issue to be noticed and resolved. Some credit card companies allow you to set a password to prevent this form of theft. Cloned cards: devices called "skimmers"; that match card readers in retail terminals can allow thieves to stealthily swipe a card number and then make a copy for illegal use. Cards with EMV chips (Europay + MasterCard + VISA) have made this process much more difficult. Cardless Theft: This is the fraudulent use of a credit card account without a physical card. Scammers can get your details through phishing or hacking, and some criminals sell card details online on the dark web. The thief does not need a physical card as online shopping only requires knowledge of your name, account number and security code (Starbuck Gerson, 2023).

Banking fraud is an area where fraud patterns are ever-changing, so the tools, techniques and other prevention measures that have been developed become obsolete and require new solutions to prevent fraud, reduce costs and fraud for the bank.

There are different types of credit card fraud, but there is no established or defined classification for these offenses to prioritize their detection.

Certain technologies are used to prevent fraud, such as the "AVS" address verification system, PIN codes, and credit check value (CVV) validation. However,

these advanced techniques are not effective enough to reduce fraud. Therefore, the development of fraud detection methods is essential (Roseline et al., 2022).

Identifying fraud is difficult because the actions and behaviors of scammers often appear legitimate. Another problem is that the number of legitimate transaction records is much higher than the number of fraudulent cases (Jha, Guillen, Westland, 2012). Such unbalanced datasets require additional data processing tools. Researchers are finding increasingly sophisticated ways to detect fraud through the development of machine learning algorithms (Cherif et al., 2023), but their practical implementation is still pending to discover.

Therefore, in order to accurately identify fraud cases, it is necessary to develop dynamic systems that can adapt to new fraud methods (Carneiro, Figueira, Costa, 2017), which means that fraud detection must develop faster than the schemes created by fraudsters.

According to Carneiro et al. (2017), the methods currently in use can be divided into two main categories: manual detection (e.g., personal identity verification) and automated detection (most commonly used data mining). When data quantities are huge, manual detection becomes less effective for a number of reasons, which is why the use of data mining technologies (or the integration of the two techniques) to detect fraud is essential. The approach proposed by these authors is the development of a risk assessment system based on machine learning techniques (Logistic Regression, Support Vector Machines and Random Forests algorithms) to evaluate fraud for each settlement on a scale of 0 to 1. Among all the authors' models, the best results were obtained with the random forest algorithm. Model validation was performed on test data.

Banking fraud is quite difficult to detect in the banking industry for one important reason: among all banking transactions, fraudulent transactions are only a small fraction of the total number of transactions, and in the overall of the numbers seem low, but an attack is enough to cost a card issuer, a fundraiser, or a merchant hundreds of thousands or even millions of dollars in losses. Therefore, they are classified as transaction anomalies. Graph-Based Anomaly Detection (GBAD) methods are used to detect these anomalies - one of the most common methods used to analyze suspicious behavior in communication services supply companies, which can also be equated with suspicious behavior when paying with bank cards. Pourhabibia, Ongb, Kama and Boo, (2020) in their article analyzed the application of different GBAD methods in detecting fraud published in scientific articles in the period 2007-2018. Furthermore, in their study, these authors sought to explore current trends and identify key challenges that require significant research. In recent years, GBAD methods have made a significant contribution to fraud detection, and

fraud detection experts have recognized them as suitable, reliable and promising methods for detecting anomalies (Velampalli & Eberle, 2017).

Mason and Bohm, (2017) in their article "Bank and Fraud" indicate that the methods used by fraudsters to take advantage of bank customers have improved significantly. Therefore, in September 2016, the British magazine What?, submitted a complaint to the Payment Regulator asking it to formally investigate bank transfer fraud and to assess the cost of preventing it to users, as well as to propose new ways and means to maximize the protection of bank customers from forced money transfers. The authors state that the methods used by fraudsters are still relevant today, and their recommendations can be summarized as follows: the government needs to change the regulations on how it handles reports of theft from bank accounts; the police departments must notify their officers of criminal activities in the digital space; banks must adopt more stricter methods to ensure the safety of customer accounts.

D. Olszewski (2014) to detect fraud suggests to use Kohonen neural networks, namely the Self-Organizing Map (SOM). The advantage of this method is that it is a general fraud detection method - it is not focused on a specific domain or application and can be easily adapted to any information system that collects data from sequential user actions, such as banking transactions. This proposed approach is distinguished by the use of an unsupervised fraud detection method, namely Unsupervised Learning, which avoids the problems of insufficient training of the data, which has an impact on the supervised data mining methods when the final results are obtained.

S. Jha et al. (2012) study the existence of insufficient academic literature on the detection of fraud in banking. To detect bank card fraud, they recommend transaction aggregation, which captures merchant's behavior before each transaction and uses these aggregations to model estimation to identify fraudulent transactions. Fraud detection is an ongoing activity as it is impossible to know whether fraud has been prevented and which transactions are fraudulent (Jha et al., 2012).

In their study, a logistic model that uses primary and derived attributes was estimated. Additional (derived) attributes were created based on the aggregation of transaction values in different time periods. Transaction aggregation was found to be a good strategy for fraud detection as the model developed with the derived attributes performed well in the classification approach. The study shows that the logistic model is appropriate, but the overall percentage of correctly classified cases is not a good indicator for classification, where the number of legitimate transactions is much higher than the number of fraud cases. For example, in a dataset with 500 fraud cases and 50 million legitimate transactions, the detection method correctly identified 495 fraud transactions, but 500 000 legitimate transactions were flagged as fraud. In other

words, the supposedly 99% accurate detection method incorrectly identified more than 1000 legitimate transactions as fraud for every correctly identified fraudulent transaction.

Linear discriminant analysis functions are less sophisticated classifiers compared to the others discussed above, which can also solve large scale problems and can be used for fraud detection credit cards, but this particular approach has not received much attention in the scientific literature. In their study, they were the first to apply Fisher's discriminant function to detect fraud (Mahmoudi & Duman, 2015). An implemented modification of the descriptive method individually estimates certain weights of transactions, to which the linear classifier tries to assign accurate labels to transactions with higher importance/priority. To summarize the results of these researchers, it can be said that the adapted method, not just based on classical performance indicators, gave good results in the detecting credit card fraud. Therefore, this method can correctly flag transactions with a high bank card limits, helping to avoid high banking costs in real systems.

A. Eshghi and M. Kargari (2019) in the paper "Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty" propose an innovative method for fraud detection. They argue that there is a some cognitive uncertainty in the detection of credit card fraud, i.e. a lack of information about various aspects of customer behavior, leading to fraud detection outcomes and thus to an inefficient application of fraud detection in the real world. They propose to address this uncertainty by using a multi-criteria solution and Fuzzy Logic approach. The behavior of the transactions was modelled taking into account the different trends of the underlying and aggregated variables at different periods. In this way, the behavior of transactions was modelled in terms of the trends of the different underlying and aggregated variables over different time periods, and the extent to which a new transaction deviated from each of these trends was considered as evidence of behavior.

Big data real-time processing is a serious problem that not all fraud detection systems are capable of handling huge amounts of data. Therefore, in this work, F. Carcillo et al. (2018) presented the Scalable Real-Time Fraud Finder (SCARFF) system, which combines big data tools with the machine learning techniques. Such a framework addresses imbalances, non-stationary and feedback. Experimental studies carried out by researchers have confirmed that the developed system is scalable, efficient and sufficiently accurate in detecting fraud (Carcillo, Pozzolo, Le Borgne, Caelen, Mazzer, & Bontempi, 2018).

In 2014, N. S. Halvaiee and M. K. Akbari conducted scientific research in which he analyzed models and methods suitable for the prevention of bank card fraud cases. According to them, Artificial Immune Systems (AIS) could be used to address such

problems. However, financial organizations and banks need accuracy and fastness in fraud detection systems, which are not yet fully realized. To address this problem, researchers have used AIS and developed the AIS-based Fraud Detection Model (AFDM). They also used an AIRS-based algorithm whose parameters were improved, i.e. the accuracy of the result was increased to 25%, its cost was reduced to 85% and the response time of the system was reduced to 40% compared to the baseline (unmodified) algorithm (Halvaiee & Akbari, 2014).

According to Attigeri et al. (2018), the transition from a traditional to a cashless economy requires banks to have more anti-fraud systems. To understand and transform the needs of the banking system, it is necessary to understand the fraud landscape and build a fraud knowledge base. In this case, the knowledge could be automatically integrated into the system to combat fraud. The work of these researchers focuses on the analysis of existing fraud case documentation. LDA (Latent Dirichlet Allocation) topic modelling was used to calculate the TF-IDF (Term Frequency-Inverse Document Frequency) weighting in order to identify a group of words (topics) describing a particular type of fraud. Using these knowledge bases, an extracted ontology can be used to construct the fraud detection system (Carcillo et al., 2018).

Psychological portrait of the victim of fraud with bank cards

Of course, not every person will fall for the psychological trick of a fraudster, and many are able to withstand criminal attacks. Experts note that older people or women are more often caught in the network of scammers.

The main personality traits that increase the risk of becoming a victim of fraud with a bank card: a thirst for freebies, personal immaturity, a craving for the amazing or even miraculous.

The first and most important attitude of the victim to “freebies” is that the person is, as it were, ready to be deceived by the very attitude to gratuitousness, i.e. the desire for "freebies" - the desire for easy money, quick and easy benefits. This is a kind of "passive stealing" that makes the victim a potential accomplice in the scam. It manifests itself as begging, wandering, dwelling, begging, etc. The "begging behavior" is widespread in different animal species. This begging phenomenon is studied by sociologists, biologists and behavioral specialists.

Another feature of the victim's personality, which is fertile ground for fraud, is some personal immaturity, expressed in curiosity, gullibility, excessive gullibility, naivety, increased anxiety, lack of proper guidance of the mind and sober rationality.

Of course, this is primarily due to the impulsiveness of actions and insufficient rationality, i.e. guided by the principle of "first did - then thought."

Another personality trait that unites victims of fraud is the desire of a person for something unusual, amazing or even wonderful. Belief in a "miracle" is characteristic of all children, but adults often sin with excessive naivety, most likely this is another facet of personal immaturity.

Research methodology

Financial criminals use a variety of scams to extort money and, increasingly sophisticated, victims often hand over their money to fraudsters voluntarily - without any hacking or violence involved. The aim of the study was to find out the knowledge of the academic community about financial fraud methods and how to prevent them.

A quantitative survey was conducted in a 2022, and 308 questionnaires were completed. The study involved staff and students from higher education institutions. Respondents received a questionnaire consisting of 10 questions. The questions were both closed and open, allowing for more detailed answers and more reliable information.

The survey included 195 women and 113 men. Most of the respondents were students, so the 18-30 age group accounted for the highest percentage (83 %). The distribution of other respondents, who are academic staff, is as follows: age group 30-40 years old - 4%, age group 40-50 - 8%, and 50 years and older - 5%. Students and professors of social sciences and technology were interviewed.

Research Results

Those surveyed have not encountered fraud, but 83% have heard of such cases. Young respondents have heard about it from social networks, middle-aged respondents - from the media, social networks. 10% of the respondents looked for information on the Internet, or in bank departments.

The most common fraud methods have been mentioned: payment card data theft, advertising site scams, investment scams, phishing, smishing and even romantic cheating. Majority (74.5%) of the respondents said they had heard of all of these fraud/cheating methods, but a quarter (25.5%) had not heard of all of them.

By next block of questions, we wanted to find out the respondents' knowledge about fraud related to bank cards. Questions that were asked: Can fraudsters steal card data at a great distance, Can fraudsters steal data at close range, and can fraudsters steal card data from a distance - 11.8%. Respondents believe that data can

be stolen over a long distance. 21.2% - theft is possible when the fraudsters are very close, the rest either do not know or think that this method of theft is not possible.

After examining the distribution of responses by age group, it was found that older respondents were convinced that such methods of theft were possible.

After surveying the respondents, in which ways they carry out payments, 78% use contactless payment, 17% - smartphones.

70% of respondents believe that the contactless payment method is safe, 5% - it partially safe, 25% have no opinion about it.

The following block of questions was used to find out the knowledge and opinion of the respondents about "fraud on advertising websites". When respondents were asked how they think such a theft compares to other financial frauds, the respondents think they are big or very big. During and after the pandemic, with the increase in online commerce, this method of fraud is becoming one of the most popular. Several respondents have encountered this type of fraud, 21% has encountered indirectly but in a close environment (relatives, relatives, friends, acquaintances, etc.) 74% are trying to be very careful when shopping on the Internet, communicating with sellers of goods sold through advertisements.

Phishing and smishing have been heard by 30% of the respondents, most of them are 18-30 year old. To the question related to these terms "Have you received an SMS message and a link from the bank or a call that something is happening with your account and you need to log in urgently". About 8% have received such messages, 70% have heard from their close friends about such messages or calls from the bank. 95% of respondents believe that they would not trust such messages and would not fall into the traps of fraudsters. Respondents watch, read the stories of victims of fraudsters and think - "this will not happen to me".

The respondents who took part in the survey were aware of this type of "Romantic Cheating" and name it as "frauds of naive or single women... frauds of single people looking for love... frauds of older women... and others." Not a single survey participant has suffered financially as a result of such fraud, but 73% of respondents have received offers to meet, make friends, communicate on social networks from foreign men, mostly from: Asian countries, the United States of America, presenting themselves as officers, engineers, etc. 85% don't even respond to inquiries 15% respond to messages out of curiosity, but they are confident that they can identify fraudsters or fraudsters.

Conclusions

Summarizing the ideas of the scientists and the briefly described results of the research presented and survey conducted, it can be said that the problem of fraud

detection is still relevant, despite the information that is given through the media to people about fraud and how to avoid it, despite the systems that used, developed methods and modified algorithms, a topic that has not been fully analyzed; there are certain uncertainties that prevent a proper assessment of the effectiveness of the proposed methods or solutions: lack of publicly available data and lack of conducted scientific research, i.e. most of the literature on the topic of credit card fraud detection focuses only on classification models.

Despite the lack of fully reliable methods and tools to date, it is hoped that in the future advanced systems will become available to detect and prevent bank card fraud at an early stage and community be informed and prepared to such dangerous cases much better than now.

A brief overview of the human factors influencing behavior shows that scammers are clever at using social engineering techniques, whereas psychology being one of the main tools.

Fraud is always uncontrollable stress for the victim. Thus, the psychological basis of any fraud with plastic cards, where the victim is the object of the crime and takes active steps that lead to the loss of his money, is an uncontrollable stressful situation.

After conducting research (academic community) on the topic of financial fraud, it can be concluded that representatives of the academic community have knowledge of financial crimes and different forms, the most famous forms of crime are: theft of payment card data, fraud on advertising sites, romantic cheating. Less known or otherwise called: investment fraud, phishing and smishing. The most common form of financial fraud at the moment is called advertisement fraud, which is believed to be related to the rise of online commerce during the pandemic. Respondents receive the most information from the media and social networks and from the circle of relatives.

Representatives of the academic society relies on its knowledge of financial crimes and believes that it is difficult or impossible for fraudsters to defraud, but it is assumed that respondents look, read the stories of victims of fraud and think - "this will not happen to me", the reality is different, as more and more new victims appear and representatives of this community.

The rise of financial fraud is a global phenomenon and the Baltic countries are no exception. Therefore, elementary knowledge of the most common methods of enticing money at the moment will help you to be more alert and recognize fraudsters who are trying to steal money. It is proposed to introduce separate topics about fraud cases in educational institutions, in relevant lectures/lessons related to economic/financial education, to provide knowledge on how fraud works on the Internet/computer technologies through technology classes.

References

An official website of the United States government. Retrieved from: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/credit-card-fraud

Carcillo, F., Pozzolo, A. D., Le Borgne, Y.-A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). Scarff: A scalable framework for streaming credit card fraud detection with spark. *Information Fusion, 41,* 182-194.

Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining based system for credit-card fraud detection in e-tail. *Decision Support Systems, 95.* Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0167923617300027#ab0005

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud *University – Computer and Information Sciences, 35,* 145-174.

Eshghi, A., & Kargari, M. (2019). Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty. *Expert Systems with Applications, 121*.

Experian Information Solutions. (n.d). Retrieved from: https://www.experian.com/

Halvaiee, N. S., & Akbari, M. K. (2014) A novel model for credit card fraud detection using Artificial Immune Systems. *Applied Soft Computing, 24*, 40–49.

Jha, S., Guillen, M., & Westland, J. C. (2012). Employing transaction aggregation strategy to detect credit card fraud. *Expert systems with applications*, *39*(16), 12650-12657.

Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified Fisher discriminant analysis. *Expert Systems with Applications*, *42*(5), 2510-2516.

Mason, S., & Bohm, N. (2017). Banking and fraud. *Computer Law & Securit review 33*(2), 237-241.

Olszewski, D. (2014). Fraud detection using self-organizing map visualizing the user profiles. *Knowledge-Based Systems, 70,* 324–334.

Pourhabibia, T., Ongb, K.-L., Kama, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems, 133,* 113303.

Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach. *Computers and Electrical Engineering*, *102*, 108132.

Starbuck Gerson, E. (2023*).* Steps to Take if You Are the Victim of Credit Card Fraud. Retrieved from: https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/credit-card-fraud-what-to-do-if-you-are-a-victim/

Velampalli, S., Eberle, W. (2017). Novel graph based anomaly detection using background knowledge. *Proceedings of flairs, AAAI Press*.