ENSURING CYBERSECURITY IN BANKING CARDS: GLOBAL RISK TRANSFORMATION AND FOREIGN MODELS

Mokhichehra Kurbonbekova
Doctor of Economic Sciences (DSc),
Associate Professor, Department of Banking,
Tashkent State University of Economics
Email: mohichehra89@list.ru
ORCID: 0000-0002-0779-2632

Guzal Mamadiyarova
Junior Researcher, Tashkent State University of Economics
Email: guzalmamadiyarova@gmail.com
ORCID: 0009-0000-4822-4044

Abstract: This article examines the issue of ensuring cybersecurity in banking card systems from the perspective of global risk transformation. In the context of the digital economy, payment infrastructure is evolving into not only a technological domain but also a strategic risk center. Drawing on the models of the United States, the European Union, Singapore, and Japan, the study explores cyber risk management architecture, institutional coordination, proactive monitoring systems, and the concept of digital trust. The paper proposes an integrated model for ensuring banking card security based on the formula "technology + regulation + risk analytics + human capital."

Keywords: cybersecurity, banking card security, digital payment systems, EMV technology, Strong Customer Authentication (SCA), fraud monitoring, artificial intelligence, risk management, skimming.

Introduction

The financial system of the twenty-first century has entered a stage of digital transformation. In a context where cash circulation is declining and online commerce and electronic services are developing rapidly, bank cards have become a central element of the global payment infrastructure. Previously, bank cards were primarily used for withdrawing cash from ATMs or making payments at retail outlets. Today, however, they have become part of a complex ecosystem closely connected with electronic commerce, international cross-border settlements, fintech platforms, mobile applications, and digital identification systems.

In the context of the digital economy, bank cards are not merely financial instruments but also key components of data flows, identification mechanisms, and trust architecture. Therefore, cybersecurity in bank card systems should not be viewed solely as a technical protection measure, but as a strategic factor of economic stability.

Over the past decade, the share of cashless transactions has increased sharply worldwide. The growth of electronic payments accelerated even further during the pandemic period. Contactless payments, online purchases, and mobile banking services developed rapidly. This process expanded financial inclusion, increased economic activity, and reduced transaction costs. However, the expansion of digital infrastructure has also generated new forms of cybercrime.

The evolution of cyber threats has progressed from traditional fraud to sophisticated and automated forms of cybercrime. During the era of magnetic stripe cards, the main threat was physical skimming. Today, however, threats such as phishing, malware, ransomware, large-scale database breaches, botnet networks, and even AI-driven automated attacks have become dominant. Bank card data have become a commodity traded on dark web markets and are distributed through transnational criminal networks.

From this perspective, ensuring cybersecurity in bank cards involves several interconnected factors:

- technological protection mechanisms;
- legal regulation;
- institutional coordination;
- risk management;
- the human factor.

The experience of developed countries demonstrates different models in this field. In the United States, market mechanisms and private sector initiatives play a dominant role, and PCI DSS standards together with real-time monitoring systems are widely applied. In the European Union, strict regulatory requirements such as PSD2 and Strong Customer Authentication have been introduced. In the United Kingdom, the Open Banking platform has elevated payment system security to a new level. In Japan, a centralized coordination model based on cooperation between the public and private sectors has been established.

The analysis of these models indicates that there is no universal solution for ensuring bank card security. Each country adopts an approach consistent with its institutional framework, economic conditions, and level of technological development. Nevertheless, all models share a common feature—comprehensive and integrated risk management.

In modern conditions, cybersecurity should not rely solely on a defensive concept. Instead, it requires a proactive approach. This means that rather than responding only after threats occur, priority should be given to forecasting risks in advance, detecting anomalies in real time, and reducing the probability of threats.

Artificial intelligence and machine learning technologies are creating new opportunities for bank card security. Through big data analysis, it becomes possible to model transaction behavior, create user profiles, and automatically detect anomalous activities. At the same time, biometric authentication—such as fingerprint recognition, facial recognition, and voice identification—helps reduce risks associated with the human factor.

However, as technologies develop, threats also become more sophisticated. Deepfake identification, AI-generated phishing messages, and automated attacks require continuous updates of security systems. Therefore, ensuring the security of bank card systems remains a constantly evolving and dynamic process.

Review of literature on the subject

In the past decade, cybersecurity issues related to bank cards have become an increasingly significant subject of academic discussion, developing in parallel with the advancement of financial technologies. Contemporary research generally examines this field in four main directions: fraud modeling, regulatory approaches, behavioral risks, and technology–infrastructure challenges.

Böhme and Moore (2012) analyze the market mechanisms of cybercrime and emphasize that bank card data constitute highly liquid assets within the “underground economy.” According to their findings, the global trade in card data significantly increases cross-border risks.

Herley (2014) analyzes phishing attacks from an economic perspective and demonstrates that cybercriminal behavior is based on rational profit maximization. This perspective supports the strategy of increasing the cost of attacks in order to reduce risks associated with bank cards. Levitin (2018) examines the issue of regulatory balance in payment systems and highlights that consumer protection mechanisms play an important role in limiting fraud.

Gai and Qiu (2018) analyze cyber risks in financial networks using network theory and show that risks arising in one bank may spread to other institutions. This finding indicates that bank card security should also be considered from the perspective of systemic risk. Aldasoro et al. (2020) emphasize that cyber incidents can have macroeconomic implications for financial stability. Their research concludes that large-scale data breaches negatively affect market confidence.

Cavusoglu, Mishra, and Raghunathan (2004) scientifically demonstrate that investments in information security increase firm value. Xu, Hu, and Zhang (2019) analyze deep learning models in the field of credit card fraud detection and show that neural networks demonstrate high accuracy in identifying anomalous transactions.

Jurgovsky et al. (2018) experimentally confirm that recurrent neural networks are effective tools for real-time fraud detection. According to the European Central Bank (2021), the introduction of EMV technology led to a reduction in card-present fraud across Europe. The Federal Reserve (2022) reports that the increase in card-not-present fraud in the United States is largely associated with the growth of online commerce.

Bouveret (2019) argues that cyber risks can pose threats to financial stability and that regulators should adopt macroprudential approaches to address these risks. Claessens et al. (2018) emphasize that the digitalization of payment infrastructures requires the development of a new risk architecture.

Conti, Lal, and Ruj (2018) evaluate tokenization as an effective cryptographic mechanism for enhancing payment security. Kosse (2013) highlights that consumer trust in digital payments strongly depends on the level of security. Milne (2016) analyzes risks associated with data sharing in the Open Banking infrastructure and emphasizes the importance of API security.

Zhou et al. (2018) analyze mobile payment security and demonstrate the effectiveness of biometric authentication methods. Johnson (2015) highlights the decisive role of the human factor in cybersecurity management. Moore and Clayton (2017) emphasize that effective responses to cybercrime require international cooperation.

Arcuri and Brogi (2021) demonstrate the relationship between ESG principles and cybersecurity, arguing that security constitutes an integral component of corporate sustainability. Carstens (2021) notes that digital payment infrastructures have strategic importance for central bank policy.

Research methodology

This study is aimed at conducting a comprehensive analysis of cybersecurity mechanisms in bank card systems based on international experience, applying an integrated approach that combines qualitative and quantitative analytical methods. The research methodology consists of several stages, including theoretical analysis, comparative institutional examination, risk assessment, and conceptual modeling.

Analysis and results

In the context of the digital economy, bank cards have become a fundamental element of the global financial infrastructure. According to the World Bank's Global Findex data, the share of digital payments showed a significant growth trend between 2014 and 2024 (Table 1).

Table 1. Share of Digital Payments in Developed Countries (% of population)[1]

Year	USA	EU	United Kingdom	Japan	OECD average
2014	83%	78%	85%	68%	80%
2017	89%	84%	91%	73%	86%
2021	94%	90%	96%	81%	92%

[1] Source: World Bank Global Findex (2024), OECD Statistics (2024)

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 03 in March-2026
https://www.gejournal.net/index.php/IJSSIR

2024	96%	93%	98%	87%	95%

The data in Table 1 show that over a ten-year period the share of digital payments in developed countries increased on average by 15–20 percentage points. In particular, electronic transactions have become almost universal in the United Kingdom and the United States.

This trend indicates two important developments:

1. A sharp increase in the volume of bank card transactions.
2. An expansion of the potential exposure to cyber risks.

At the same time, the growth of digital transactions has been accompanied by an increase in card-related fraud cases (Table 2).

Table 2. Financial Losses from Card Fraud (USD billion)[2]

Year	USA	Europe	Japan	Global
2015	6.8	1.9	0.4	18.4
2018	9.2	2.4	0.6	24.7
2021	11.1	2.9	0.8	32.5
2023	13.8	3.4	1.1	38.6

Between 2015 and 2023, global card fraud losses increased by approximately 110 percent. This growth corresponds closely with the rapid expansion of digital payments. In particular, card-not-present (CNP) operations account for a large share of fraud cases in the United States. In the European Union, however, the growth of CNP fraud has slowed to some extent following the introduction of PSD2 and Strong Customer Authentication (SCA) (Table 3).

Table 3. Distribution of Fraud Types (%)[3]

Region	Card-Present	Card-Not-Present	Identity Theft
USA	28%	55%	17%
Europe	35%	48%	17%
Japan	42%	40%	18%

The highest risk is observed in online operations. Card-not-present transactions represent a high-risk segment due to the rapid development of e-commerce and mobile payments. This situation indicates that EMV chip technology has significantly reduced fraud in card-present transactions, while fraud has increasingly shifted to the online environment—commonly referred to as the fraud migration phenomenon (Table 4).

Table 4. Correlation Between Digital Payment Share and Fraud Indicators[4]

Indicator	Correlation coefficient (r)

[2] Source: Nilson Report (2024), ECB Fraud Statistics (2024)

[3] Source: Compiled by the authors.

[4] Source: Compiled by the authors.

22

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 03 in March-2026
https://www.gejournal.net/index.php/IJSSIR

Copyright (c) 2026 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY). To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

Digital payment share – Fraud losses	0.78
Online commerce share – CNP fraud	0.84
EMV implementation – Card-present fraud	-0.65

The correlation analysis demonstrates the following relationships:

- The growth of digital payment share is strongly positively correlated with fraud losses (r = 0.78).
- The expansion of online commerce shows an even stronger relationship with CNP fraud (r = 0.84).
- The introduction of EMV technology has contributed to reducing card-present fraud, reflected in a negative correlation.

Following the introduction of PSD2 and SCA mechanisms, certain changes were observed in the dynamics of fraud in the European Union (Table 5).

Table 5. CNP Fraud Before and After the Introduction of SCA (% growth)[5]

Period	European Union
2016–2019	+18%
2020–2023	+6%

Because SCA requirements mandate two-factor authentication, the growth rate of CNP fraud decreased approximately threefold. This demonstrates the effectiveness of regulatory mechanisms in improving payment security.

Conclusions and suggestions

The conducted theoretical and statistical analyses demonstrate that the bank card system has become a strategic element of financial infrastructure in the context of the digital economy. The sharp growth in the share of digital payments, particularly the expansion of card-not-present operations, creates new opportunities for cyber risks. Statistical data confirm that financial losses related to card fraud are increasing globally each year. This situation indicates that ensuring the security of bank cards should be considered not only as a technical issue but also from the perspective of economic stability and financial trust.

According to the results of the analysis, EMV technology has been effective in reducing fraud in card-present transactions. However, due to the phenomenon of fraud migration, risks in the online environment continue to increase. In the European Union, the introduction of PSD2 and Strong Customer Authentication (SCA) requirements has contributed to slowing the growth rate of CNP fraud, highlighting the importance of regulatory measures. At the same time, the human factor, the level of digital literacy, and social engineering attacks remain the weakest components of the security system.

Based on these findings, the following recommendations are proposed.

First, it is necessary to apply a comprehensive approach to ensuring bank card security. Technological protection mechanisms such as tokenization, biometric authentication, and real-time monitoring should be integrated with regulatory mechanisms and institutional coordination. The

[5] Source: Compiled by the authors.

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 15 Issue: 03 in March-2026
https://www.gejournal.net/index.php/IJSSIR

implementation of a single technological solution alone cannot fully address the problem.

Second, it is advisable to widely implement fraud monitoring systems based on artificial intelligence and machine learning algorithms. Real-time anomaly detection systems make it possible to minimize potential financial losses.

Third, regulators should introduce strengthened authentication standards and strictly monitor compliance with PCI DSS requirements. At the same time, it is important to develop information-sharing platforms between fintech companies and banks.

Fourth, systematic programs should be implemented to improve consumers' digital financial literacy. Preventive measures against phishing and social engineering attacks can significantly reduce risks.

Fifth, it is recommended to assess cyber threats as systemic risks and introduce macroprudential approaches. Cyber incidents may affect financial stability, and this factor should be taken into account in regulatory policy.

In general, ensuring cybersecurity in bank card systems should be based on the integration of technological, institutional, and economic factors. The experience of developed countries demonstrates that only a comprehensive and sustainable security architecture can ensure trust in digital payment systems.

List of used literature:

1. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). The drivers of cyber risk. *BIS Working Papers*, No. 865. Bank for International Settlements.
2. Arcuri, M. C., & Brogi, M. (2021). Cyber risk and ESG performance: Evidence from the financial sector. *Sustainability*, 13(18), 10243. https://doi.org/10.3390/su131810243
3. Böhme, R., & Moore, T. (2012). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 5(3–4), 123–134. https://doi.org/10.1016/j.ijcip.2012.09.002
4. Bouveret, A. (2019). Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*, WP/18/143. International Monetary Fund.
5. Carstens, A. (2021). Digital currencies and the future of the monetary system. *BIS Speech*. Bank for International Settlements.
6. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, 9(1), 69–104. https://doi.org/10.1080/10864415.2004.11044320
7. Claessens, S., Frost, J., Turner, G., & Zhu, F. (2018). Fintech credit markets around the world: Size, drivers and policy issues. *BIS Quarterly Review*, September.
8. Conti, M., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of blockchain technology. *IEEE Communications Surveys & Tutorials*, 20(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460
9. European Central Bank. (2021). *Card fraud statistics 2020*. European Central Bank.
10. Farooq, U., Tabash, M. I., Mamadiyarov, Z., Issa, S. S., & Aldawsari, S. H. (2025). Sustainable financial strategies: the role of intellectual capital in shaping corporate cash holdings. International Journal of Organizational Analysis, 1-19.
11. Federal Reserve. (2022). *FraudClassifier model annual report*. Federal Reserve System.
12. Gai, K., & Qiu, M. (2018). Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. *IEEE Transactions on Industrial Informatics*, 14(8), 3590–3598. https://doi.org/10.1109/TII.2018.2797065

13. Herley, C. (2014). The economics of phishing. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.

14. Johnson, M. E. (2015). Managing cybersecurity risk: An examination of risk perception and security investment. *Journal of Cybersecurity*, 1(1), 1–10. https://doi.org/10.1093/cybsec/tyv002

15. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234–245. https://doi.org/10.1016/j.eswa.2018.01.037

16. Kosse, A. (2013). Do newspaper articles on card fraud affect debit card usage? *Journal of Banking & Finance*, 37(12), 5382–5391. https://doi.org/10.1016/j.jbankfin.2013.04.009

17. Levitin, A. J. (2018). Pandora's digital box: The promise and perils of digital wallets. *University of Pennsylvania Law Review*, 166(2), 305–369.

18. Litamahuputty, J. V., Amiruddin, E. G., Rahim, R., Rahman, A., & Mamadiyarov, Z. (2025). Cryptocurrency Risk Management through Decision Engineering: Evaluating XRPUSD and ADAUSD Portfolio Performance. Journal of Applied Science, Engineering, Technology, and Education, 7(1), 69-81. https://doi.org/10.35877/454RI.asci3871

19. Mamadiyarov, Z., Hakimov, H., & Askarov, S. (2024). DEVELOPMENT OF RETAIL BANKING SERVICES IN THE CONTEXT OF DIGITAL TRANSFORMATION. Financial and Credit Activity Problems of Theory and Practice, 1(54), 51–67. https://doi.org/10.55643/fcaptp.1.54.2024.4288

20. Mamadiyarov, Z., & Karimov, K. (2024). Tijorat banklarida kredit riski va uni boshqarish usullari. Страховой рынок Узбекистана, 1(6), 57-60.

21. Mamadiyarov, Z. (2020). Prospects for the development of remote banking services in the context of Bank Transformation. The American Journal of Applied Sciences, 2(07), 108-118.

22. Milne, A. (2016). Competition and innovation in payment systems: The case of open banking. *Journal of Payments Strategy & Systems*, 10(4), 345–356.

23. Moore, T., & Clayton, R. (2017). The impact of public information on cybercrime markets. *Journal of Cybersecurity*, 3(2), 77–91. https://doi.org/10.1093/cybsec/tyx007

24. Ravikumar, R. N., Aarthi, S., & Mamadiyarov, Z. (2026). Mitigating Risks Through AI-Powered Fraud Detection Systems in Digital Banking. In Innovating Cost-Efficient and Scalable Business Models in the Digital Era (pp. 343-376). IGI Global Scientific Publishing.

25. Xu, Y., Hu, Y., & Zhang, C. (2019). Credit card fraud detection using deep learning. *Computers & Security*, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640

26. Zhou, T., Zhang, X., & Liu, Y. (2018). Mobile payment security and biometric authentication: A systematic review. *Information Systems Frontiers*, 20(2), 345–358. https://doi.org/10.1007/s10796-017-9762-8

27. Zokir Toshtemirovich Mamadiyarov. 2022. Risk Management in the Remote Provision of Banking Services in the Conditions of Digital Transformation of Banks. In Proceedings of the 5th International Conference on Future Networks and Distributed Systems (ICFNDS '21). Association for Computing Machinery, New York, NY, USA, 311–317. https://doi.org/10.1145/3508072.3508119

28. Zokir Toshtemirovich Mamadiyarov, Samandarboy Adhambek ugli Sulaymanov, Sarvar Anvar ugli Askarov, and Durdona Bakhtiyor kizi Uktamova. 2022. Impact of Covid-19 Pandemic on Accelerating The Digitization and Transformation of Banks. In Proceedings of the 5th International Conference on Future Networks and Distributed Systems (ICFNDS '21). Association for Computing Machinery, New York, NY, USA, 706–712. https://doi.org/10.1145/3508072.3508211