DOI: 10.55643/fcaptp.5.70.2026.5338

FINANCIAL AND CREDIT SYSTEM UNDER DIGITAL TRANSFORMATION AND CRIMINAL-LAW RISKS OF PAYMENT FRAUD

Nataliia Parasiuk
PhD in Legal Sciences, Associate Professor, Deputy Director for Education and Research Activities, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0002-7489-9181

Yuliia Lisitsyna
PhD in Legal Sciences, Associate Professor of the Department of Criminal Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0001-5631-9297

Stvitlana Romantsova
PhD in Legal Sciences, Associate Professor of the Department of Criminal Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine;
e-mail: romançova_s@ukr.net
ORCID: 0000-0003-0888-5934
(Corresponding author)

Zoriana Dilna
PhD in Legal Sciences, Associate Professor of the Department of Criminal Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0002-6066-1279

Iryna Serkevych
PhD in Legal Sciences, Associate Professor of the Department of Criminal Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0001-7678-0291

Received: 11/08/2026
Accepted: 17/10/2026
Published: 31/10/2026

© Copyright
2026 by the author(s)

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

ABSTRACT

The financial and credit system under digital transformation is characterised by the rapid expansion of cashless payments, remote banking services, and new forms of interaction between financial institutions and customers. At the same time, the nature of payment-fraud risk is changing, as a decline in the relative frequency of fraudulent transactions may coexist with increasing financial severity and a growing role of social engineering. The study aims to assess the transformation of payment-fraud risks within the financial and credit system and to determine the criminal-law significance of the identified changes amid the increasing role of remote financial services. The empirical base combines official data from the National Bank of Ukraine, the Cyber Police Department of the National Police of Ukraine, and relevant provisions of criminal legislation. The methodological approach integrates an assessment of payment-activity dynamics, additive LMDI decomposition of financial losses into frequency and average-severity effects, exposure-normalised fraud indicators, structural analysis of social engineering, and criminal-law systematisation of major risk channels. The results indicate that the expansion of payment activity is accompanied by a decline in the relative frequency of successful fraudulent transactions, while the financial severity of such incidents continues to increase. At the same time, the growing role of social engineering shifts the focus from purely technical protection of payment infrastructure towards protecting the behavioural decision-making process of users. The scientific novelty lies in adapting LMDI decomposition to payment-fraud assessment and combining it with exposure-normalised indicators and criminal-law interpretation. The practical value of the proposed approach lies in its potential use by banks, regulators, and law-enforcement authorities to jointly assess fraud frequency, financial severity, behavioural mechanisms, and potentially relevant areas of legal response.

Keywords: financial and credit system, digital transformation, payment cards, payment fraud, cyber risk, social engineering, criminal-law protection, LMDI decomposition, cashless payments

JEL Classification: G21, G23, G28, K42, O33, C43

INTRODUCTION

The financial and credit system is one of the sectors where the adoption of digital technologies is most visibly altering the way economic transactions are conducted. Bank accounts, payment cards, mobile banking, remote identification, instant transfers, and open banking increasingly facilitate the movement of funds without direct physical interaction be-tween the client and the financial institution. As a result, financial and credit relations are increasingly shifting toward remote forms of interaction, in which the initiation, authorisation, processing, and completion of payment transactions are carried out through digital channels involving banks, payment service providers, and customers.

Alongside the increased accessibility and speed of financial services, these changes are transforming the risks inherent in the financial and credit system. Payment fraud stands out as one of the most significant risks. The expansion of remote channels increases the number of touchpoints through which a criminal can obtain payment details, influence user behavior, initiate unauthorized access, or manipulate a victim into personally

authorizing a fund transfer. Thus, fraud risk emerges at the intersection of the financial transaction, the technological channel, client behavior, and the illicit method used to misappropriate funds.

A key characteristic of modern payment fraud is that its prevalence cannot be accurately assessed solely by the number of recorded illicit transactions. A decline in the number of incidents may coincide with a rise in the average loss amount, causing the aggregate financial impact of fraud to worsen. Under these conditions, relying solely on frequency creates a risk of erroneously concluding that payment security is improving. For the financial and credit system, it is crucial to consider the number of successful fraudulent transactions, the resulting financial losses, the average loss amount, and how these metrics compare to the total volume of payment activity. Changes in the methods used to execute fraudulent schemes are also of particular importance. Payment infrastructure may be technically secure, yet a user–swayed by deception, psychological pressure, information tampering, or other social engineering tactics–may voluntarily disclose credentials or authorize a financial transaction. In such a scenario, the victim's financial loss stems from an action that is formally authorized, even though the underlying intent was shaped by criminal manipulation. Thus, the technological evolution of the financial and credit system simultaneously alters the economic and criminal-law dimensions of payment fraud risk.

In our view, the focus of research should be the changing nature of the financial and credit system's operations and payment fraud risks resulting from digital transformation, rather than the digitalization process as a standalone phenomenon. This approach makes it possible to link rising payment exposure, shifts in the volume of illicit transactions, the scale of financial losses, the prevalence of social engineering, and potential avenues for criminal-law classification within a unified research framework.

LITERATURE REVIEW

The first line of research concerns changes in the financial and credit system driven by technological transformation. Domestic authors view the digitalization of the banking sector as a process encompassing shifts in business models, service channels, organizational structures, and modes of interaction between banks and clients. Andriushchenko and Skydan (2023) highlight the transition from traditional banking ecosystems to new models built around technological interaction and new managerial competencies. Artemieva and Zaliubovska (2023) examine the transformation of banks resulting from increased service speed, accessibility, and personalization, while simultaneously emphasizing the importance of security and confidentiality. Demchyshak et al. (2024) directly link technological development within the country's banking system to increased financial transaction efficiency, as well as heightened cyber risks and the likelihood of fraud. A similar general perspective is found in international literature–specifically in works by Gomber et al. (2017), Gomber et al. (2018), Boot et al. (2021), and Thakor (2020)–which view fintech as a driver of change regarding the structure of financial intermediation, transaction speed, and interactions between traditional and new financial market participants.

The second line of research relates to the expansion of remote payment infrastructure and Open Banking. Hordei and Sereda (2024) regard open banking as a key driver of change in the banking system; while it expands interaction capabilities via Open APIs, it simultaneously creates new risks and necessitates enhanced data protection. Sharenko and Dobrunova (2025) further emphasize the need for secure financial information exchange between banks and third parties, as well as the regulation of liability and personal data protection. Hrechka et al. (2025) view cybersecurity, in-formation privacy, and technological risks as components of the financial security of banking institutions.

A third area of research focuses specifically on payment fraud and its financial consequences. Liubkina and Taraba (2025) analyze the trends in fraudulent transactions within the country's payment system, highlighting social engineering, the misuse of payment infrastructure for illicit purposes, and the need for interbank cooperation. Bondaruk et al. (2023) demonstrate that the evolution of banking and payment technologies has been accompanied by the emergence of more sophisticated payment card fraud methods, and that effective countermeasures require a combination of technological safeguards and increased customer awareness. While these studies are closely aligned with our research topic, their primary focus is on fraud typologies, countermeasures, and the characteristics of payment infrastructure.

A fourth area concerns behavioral and cyber risks. Workman (2008) shows that social engineering relies on psychological mechanisms that induce users to perform actions benefiting the attacker. Vishwanath et al. (2011) link susceptibility to phishing with users' information processing styles and a lack of critical assessment regarding the messages they receive. Kopp et al. (2017) examine cyber risks in the context of financial stability, highlighting information asymmetry and externalities, whereas Kamiya et al. (2021) demonstrate that the consequences of successful cyberattacks extend beyond immediate financial losses to include reputational and market impacts.

DOI: 10.55643/fcaptp.5.70.2026.5338

A fifth area comprises research in criminal law and forensics. Usmanov (2024) analyzes fraud committed through illicit operations involving electronic computing technology and highlights the difficulty of establishing deception in situations where an illegal payment is mediated by an automated banking system. Shapoval et al. (2021) examine efforts to counter offenses involving electronic payment systems and emphasize the need to combine legal, organizational, and technological measures. Bondaruk et al. (2023) also draw attention to the subsequent movement of funds via payment instruments, while Levi and Reuter (2006), within the broader context of financial monitoring, note the importance of tracking illicit financial flows.

The sixth area concerns the quantitative decomposition of changes in an aggregate result into individual factors. Ang (2015) characterizes the additive LMDI approach as a method for the exact decomposition of changes in a resultant indicator, without a residual term. While traditional studies primarily employ LMDI to assess energy and environmental indicators, its mathematical structure does not restrict its application to any specific sector.

AIMS AND OBJECTIVES

The study aims to assess the transformation of payment fraud risk within the financial and credit system by distinguishing between the frequency of illicit transactions and the severity of financial losses, as well as to determine the criminal-legal significance of the observed changes amidst the growing role of remote financial services. The specific objectives are to:

- systematize the dynamics of payment exposure in terms of the volume and value of card transactions during 2023–2025;
- evaluate changes in the number of illicit transactions, total losses, the average value per fraudulent transaction, and the share of social engineering incidents during 2022–2025;
- apply LMDI decomposition to the increase in total losses and determine the respective contributions of the frequency effect and the severity effect;
- compare normalized fraud frequency and normalized financial severity relative to payment exposure;
- cross-reference the obtained data with selected aspects of criminal-legal protection and cyber-police performance indicators for 2024–2025.

METHODS

The empirical period covers the years 2022–2025. This timeframe was selected due to the availability of comparable annual data on fraudulent payment card transactions and the ability to track changes in the risk structure following the onset of the full-scale war. Figures for total payment turnover for 2022 were excluded from the normalized assessment, as the National Bank explicitly notes the incompleteness of statistical reporting for February–April 2022. Consequently, completed and comparable annual data for 2023–2025 were used for payment exposure, while data for 2022–2025 were used for fraud loss dynamics. The information base comprises three groups of official data. The first group covers National Bank statistics on the volume and value of payment card transactions, the share of cashless payments, and the number of active cards and payment terminals. The second group contains indicators of illicit activities and fraudulent payment card transactions–specifically the number of transactions, total losses, average value per illicit transaction, relative frequency of fraudulent transactions, relative loss rate, and the share of social engineering. The third group covers reports from the Cyber Police Department for 2024–2025 regarding registered criminal offenses, notices of suspicion, cases referred to court, and recovered damages. The normative basis for the substantive interpretation consists of the current provisions of the Criminal Code of Ukraine and the National Bank's regulations regarding open banking, strong authentication, and the cyber-protection of the payment market.

The analytical total loss is calculated as the product of the number of fraudulent transactions resulting in a recorded loss and the average loss amount per such transaction. Since official annual figures are published in rounded form, the calculated product may differ slightly from the total loss volume reported by the regulator (1–2):

$$L_t = N_t \times A_t, \quad (1)$$

where L_t is the analytical fraud loss in year t; N_t is the number of loss-generating fraudulent transactions; A_t is the average loss per fraudulent transaction.

$$A_t = \frac{L_t}{N_t}, \quad (2)$$

where A_t is expressed in UAH per fraudulent transaction; the units of L_t and N_t are harmonised before calculation.

The second stage involves the additive LMDI decomposition of the change in the analytical sum of losses between two consecutive years. Unlike a simple comparison of growth rates, this approach reveals the absolute contribution of each factor in million UAH (3–6):

$$M(L_t,\ L_{t-1}) = \frac{L_t - L_{t-1}}{\ln(L_t) - \ln(L_{t-1})}, \quad (3)$$

where M is the logarithmic mean used as the additive decomposition weight.

$$\Delta L_t^N = M(L_t, L_{t-1}) \ln\left(\frac{N_t}{N_{t-1}}\right), \quad (4)$$

where ΔL^N is the frequency effect expressed in UAH million.

$$\Delta L_t^A = M(L_t, L_{t-1}) \ln\left(\frac{A_t}{A_{t-1}}\right), \quad (5)$$

where ΔL^A is the severity effect expressed in UAH million.

$$\Delta L_t = \Delta L_t^N + \Delta L_t^A, \quad (6)$$

where ΔL is the total change in analytical fraud losses between two consecutive years.

The third stage aims to eliminate the impact of the expansion of payment turnover itself. Two normalized indicators are used for this purpose. The first characterizes the number of fraudulent transactions per 1 million outgoing payment card transactions. The second reflects the amount of losses (in UAH) per 1 million UAH of outgoing card turnover. Values published by the regulator were used for 2024–2025. The 2023 benchmarks were reconstructed based on officially published relative changes for 2024–an 8% decrease in frequency and a 28% increase in relative losses (7–8):

$$\mathrm{FED}_t = \frac{N_t}{T_t} \times 10^6, \quad (7)$$

where FED_t is fraud event density; T_t is the number of expenditure payment-card transactions.

$$\mathrm{FLD}_t = \frac{L_t}{V_t} \times 10^6, \quad (8)$$

where FLD_t is fraud loss density in UAH per UAH 1 million of expenditure turnover; V_t is the value of expenditure payment-card transactions.

The fourth stage involves a structural comparison of the share of losses caused by social engineering. This indicator is not included in the aggregate index and is not used to establish causality. It characterizes the shift in the dominant loss mechanism and is considered alongside the LMDI results (9):

$$s_t = s_t - s_{t-1}, \quad (9)$$

where s_t is the share of total fraud losses attributed to social engineering in year t, %.

RESULTS

Between 2023 and 2025, the number of payment card transactions increased from 7.9 billion to 9.5 billion, while their total value rose from UAH 6.14 trillion to UAH 7.16 trillion. The number of cashless transactions grew even more rapidly, exceeding 9.0 billion in 2025. The share of cashless transactions (by volume) rose from 93.5% to 95.5%. Concurrently, the number of active cards increased from 52.1 million to 65.4 million, and the payment terminal network expanded from

DOI: 10.55643/fcaptp.5.70.2026.5338

449.5 thousand to 558.6 thousand units. These trends indicate that criminal-law risks exist within an environment characterized by a steadily increasing annual volume of remote and card-based financial interactions (Table 1).

Table 1. Digital payment exposure in the financial and credit system, 2023–2025. *(Source: authors' compilation based on National Bank of Ukraine payment-card statistics for 2023–2025)*

Year	Total card transactions, million	Total card value, UAH billion	Cashless transactions, million	Cashless value, UAH billion	Cashless share by count, %	Active cards, million	POS terminals, thousand
2023	7,912.5	6,14.8	7,397.2	3,98	93.5	52.1	449.5
2024	8,654.4	6,577.4	8,184.8	4,243.5	94.6	58.8	496.6
2025	9,512.3	7,157.2	9,083.5	4,684.3	95.5	65.4	558.6

Against the backdrop of expanding payment activity, the absolute trends in fraud have been mixed. In 2023, the number of illicit transactions resulting in losses rose by approximately a quarter compared to 2022, reaching 272,000. Subsequently, the figure declined to 270,000 in 2024 and 256,000 in 2025. However, the total value of losses moved in the opposite direction. It amounted to approximately UAH 481 million in 2022, UAH 833 million in 2023, over UAH 1.1 billion in 2024, and around UAH 1.4 billion in 2025. Over the four-year period, the average value of a single illicit transaction increased from UAH 2,200 to UAH 5,536 (Table 2).

Table 2. Payment-card fraud profile, 2022–2025. *(Source: authors' compilation based on National Bank of Ukraine and national payment-security campaign materials)*

Year	Loss-generating fraud transactions, thousand	Reported losses, UAH million	Average loss per fraud transaction, UAH	Social engineering share of losses, %	Internet share of fraud count, %
2022	217.6	481	2,2	53	86
2023	272	833	3,065	80	83
2024	270	1,1	4,247	84	83
2025	256	1,4	5,536	90	83

During 2022–2023, the increase in analytical losses of UAH 354.96 million was driven by a combination of factors. The frequency effect accounted for UAH 142.78 million (40.23% of the increase), while the severity effect accounted for UAH 212.18 million (59.77%). However, the structure changed fundamentally during 2023–2024. The total increase of UAH 313.01 million was driven by a severity effect of UAH 320.26 million, whereas a reduction in the number of cases offset UAH 7.25 million. In 2024–2025, the severity effect reached UAH 338.53 million, while the negative frequency effect amounted to UAH 68.00 million. The severity effect's share exceeds 100% in the last two periods because the reduction in the number of cases acts in the opposite direction, partially tempering the overall rise in losses (Figure 1).

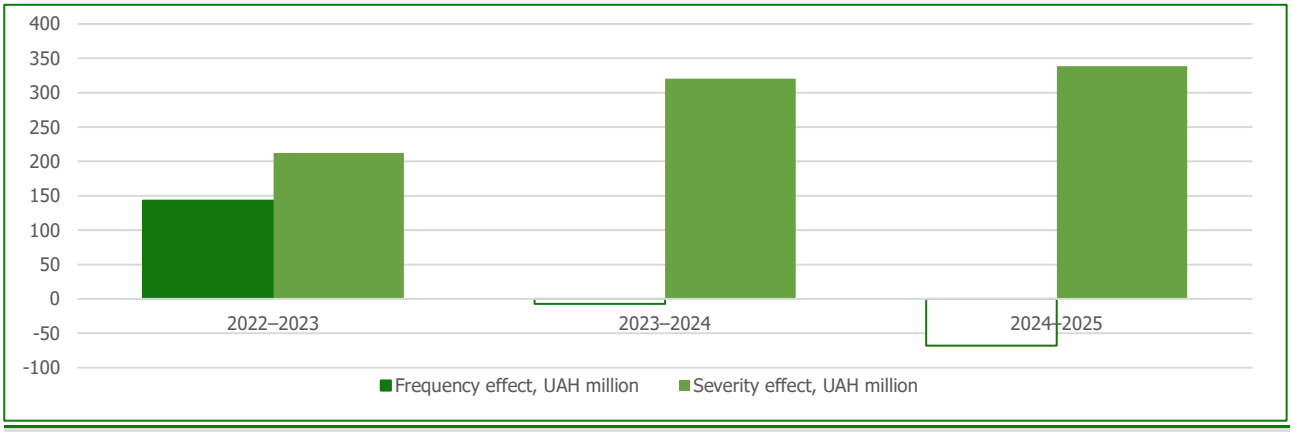


Figure 1. LMDI decomposition of payment-card fraud loss changes.

Normalizing against payment exposure confirms the same result. The number of fraudulent transactions per million outgoing transactions decreased from approximately 33.7 in 2023 to 31 in 2024 and 27 in 2025. Conversely, losses per million UAH of outgoing card turnover rose from approximately UAH 137.5 in 2023 to UAH 176 in 2024 and UAH 198 in 2025.

ISSN: 2306-4994 | eISSN: 2310-8770 | Том 5 (70), 2026

Thus, frequency risk relative to the volume of payment activity is declining, while the severity in monetary terms continues to rise (Table 3).

Table 3. Exposure-normalised payment-card fraud indicators. *(Source: authors' calculations based on National Bank of Ukraine releases)*

Year	Fraudulent transactions per 1 million expenditure transactions	Fraud losses per UAH 1 million of expenditure turnover	Interpretation
2023	33.7	137.5	Higher frequency, lower loss density
2024	31	176	Frequency declines, loss density rises
2025	27	198	Lower frequency, highest loss density

The structural indicator for social engineering illustrates the shifting trend of successful fraud. Its share of total losses stood at 53% in 2022, 80% in 2023, 84% in 2024, and–according to published estimates–approximately 90% in 2025. This represents a 37-percentage-point increase over the four-year period. The largest annual surge occurred in 2023, at 27 percentage points. While the rate of growth slowed in subsequent years, it proceeded from an already very high baseline (Figure 2).

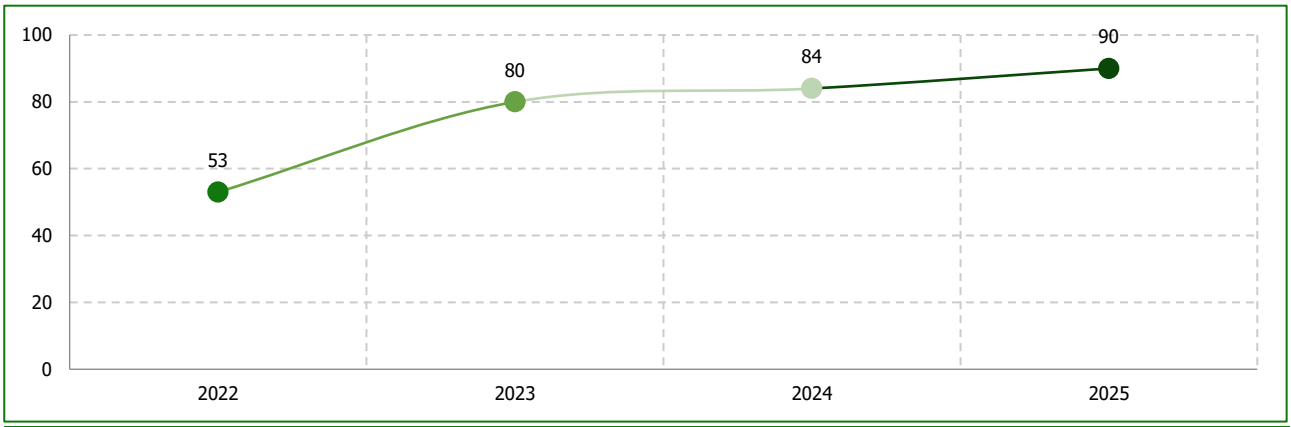


Figure 2. Share of payment-card fraud losses attributed to social engineering, 2022–2025. *(Source: authors' compilation based on National Bank of Ukraine and payment-security campaign materials)*

It is important to correlate the obtained result with criminal law avenues of protection. The statistical category of an illegal or fraudulent transaction does not automatically determine a specific article of the Criminal Code. Factual circumstances may indicate misappropriation of property through deceit, illegal actions involving payment instruments or account access, unauthorized interference with information systems, unlawful dissemination of restricted information, or the subsequent laundering of the obtained property. Therefore, it is advisable to use a potential relevance matrix rather than unequivocally equating all transactions with a single type of offense (Table 4).

Table 4. Criminal-law relevance of major digital payment-fraud channels. *(Source: authors' systematisation based on the Criminal Code of Ukraine)*

Risk channel	Typical financial manifestation	Potentially relevant Criminal Code provisions	Key evidentiary focus
Deception and social engineering	Victim authorises transfer or discloses credentials	Art. 190	Deception, abuse of trust, causal link to transfer and loss
Illegal use or handling of payment access instruments	Card/account credentials are unlawfully created, acquired, used, or transferred	Art. 200; depending on facts, Art. 190	Origin and use of payment credentials, device and account traces
Unauthorised interference in information systems	Access, alteration, blocking, leakage or disruption affects payment processing	Arts. 361, 361-1; depending on facts, Art. 362	Access logs, system integrity, malware/tools, permissions
Unauthorised distribution of restricted information	Protected account or authentication data are unlawfully sold or distributed	Art. 361-2	Status of information, access rights, transfer/distribution evidence
Subsequent movement or concealment of criminal proceeds	Funds are layered, converted, transferred through accounts or assets	Art. 209 where statutory elements are met	Source of assets, knowledge, transaction chain and concealment actions

DOI: 10.55643/fcaptp.5.70.2026.5338

The results of the Cyber Police's operations in 2024–2025 represent a distinct statistical dataset; therefore, they were not arithmetically combined with banking fraud statistics. In 2025, Cyber Police units recorded over 2,100 criminal offenses, compared to 2,500 in 2024; notices of suspicion were issued to approximately 1,500 individuals, down from 1,700; and over 2,700 cases were referred to court with indictments, compared to over 4,000 previously. At the same time, the amount of recovered damages rose from UAH 168.5 million to UAH 342.6 million, while the recovery rate–representing the proportion of damages recouped–increased from 42.5% to 70.9%. Thus, despite a lower number of recorded offenses, both the absolute amount and the relative share of recovered damages increased significantly.

In 2025, the regulatory framework defined the roles of ASPSPs, PISPs, and AISPs, as well as requirements for the authorization of non-financial payment service providers, qualified open banking certificates, specialized APIs, strong customer authentication, and information security. From the perspective of criminal law assessment, this architecture is significant due to the clearer distinction it draws between legitimate and unauthorized access. When account access occurs via a designated API–with user consent and through an authorized entity–digital event logs and certificates can enhance the evidentiary value of technical traces. At the same time, the criminal modus operandi may shift toward obtaining consent through deception, compromising the user, or using stolen credentials.

DISCUSSION

The first aspect of the discussion concerns the transformation of the financial and credit system itself. Andryushchenko and Skidan (2023), Artemieva and Zaliubovska (2023), and Demkhikhak et al. (2024) demonstrate that the development of banking technologies alters service structures, interaction channels, and security requirements. Our results support this view, given the actual expansion of payment activity observed between 2023 and 2025. Crucially, the growth in the volume and value of transactions is not accompanied by a proportional increase in the relative frequency of fraud. Con-sequently, the mere fact of technological expansion within the financial and credit system should not automatically be interpreted as an increase in the likelihood of a successful fraudulent transaction.

The second aspect relates to the relationship between the frequency and financial severity of fraud. Liubkina and Taraba (2025) and Bondaruk et al. (2023) provide a detailed characterization of the prevalence of fraudulent schemes, their link to payment infrastructure, and the need for improved countermeasures. Our results complement these studies by quantitatively distinguishing between two different sources of changes in financial losses. LMDI decomposition revealed that, early in the study period, the rise in losses was driven by both the frequency and the average magnitude of losses; in subsequent years, however, a decline in the number of successful fraud cases helped curb aggregate losses, though it failed to offset the rapid increase in their average severity.

The third aspect concerns the behavioral mechanism underlying fraud. Findings regarding the growing role of social engineering align with the conclusions of Workman (2008) and Vishwanath et al. (2011), who link the effectiveness of phishing and manipulative schemes to user decision-making processes. At the same time, our study highlights the financial implications of this shift. The rising prevalence of social engineering coincides with an increase in the average financial impact of successful fraudulent transactions. Consequently, technical authentication alone cannot fully meet user protection needs when a payment is personally authorized by the user under the influence of deception. In our view, this trend necessitates combining technological safeguards with behavioral warnings, additional scrutiny of atypical transactions, and rapid response mechanisms for fraud reports.

A fourth aspect concerns the criminal-law interpretation of the identified trends. Usmanov (2024) demonstrates the difficulty of defining deception in illicit transactions mediated by electronic systems, while Shapoval et al. (2021) highlight the complexity of combating offenses in the electronic payment sector. Our findings confirm that it is inappropriate to automatically classify the entire statistical aggregate of payment fraud under a single criminal-law provision. Social engi-neering, the illicit use of payment details, unauthorized interference with information systems, the dissemination of pro-tected information, and the subsequent movement of criminally obtained funds each entail distinct legal elements. The proposed approach differs by employing a matrix of potential criminal-law relevance that links the financial manifestation of risk to the actual method of committing the unlawful act, without supplanting individual legal qualification. Regarding the military context, the findings align with the broader position held by Kryshtanovych et al. (2023) concerning the in-terdependence of the economic and legal consequences of external destabilization. Ivashova et al. (2022) also highlight the need to adapt management processes to changes in the external environment. Within the country's financial and credit system, this dependency manifests through the simultaneous rise of remote financial channels and the emergence of new scenarios for manipulating users. However, the results do not allow for attributing the increase in financial losses solely to the war

or to digital transformation, as aggregated annual data do not permit the isolation of the causal contri-bution of each individual factor.

The study's scientific novelty lies in the development of a methodological approach to assessing payment fraud risk within the financial and credit system by sequentially combining four analytical components. First, overall payment exposure is assessed. Second, aggregate losses are decomposed–using additive LMDI decomposition–into a frequency effect and an average financial severity effect. Third, fraud metrics are normalized against the volume and value of payment transactions, thereby eliminating the impact of the mere expansion of payment turnover. Fourth, quantitative results are correlated with the structural role of social engineering and potentially relevant aspects of criminal law protection. Unlike existing studies–which typically examine digital transformation, fraud, behavioral vulnerability, and legal classification in isolation–the proposed approach integrates these elements around the financial outcome of the fraudulent transaction.

The limitations of the findings are determined by the nature of the data used. Data on total payment turnover for 2022 are incomplete; consequently, normalized indicators are calculated only for the 2023–2025 period. Official annual figures regarding the number of transactions, average loss, and total loss volume are published in rounded form; consequently, the analytical product may differ slightly from the regulatory total. Data from the cyber police represent a different statistical dataset and therefore cannot be arithmetically combined with banking statistics. Aggregated data do not allow for establishing a causal link between a specific technology, a type of social engineering, and the specific amount of a loss. The proposed criminal law matrix outlines the potential relevance of legal provisions but does not replace the legal classification of a specific criminal offense based on all the factual circumstances.

CONCLUSIONS

Regarding the first objective, a continued expansion of the financial and credit system's payment exposure was observed over the 2023–2025 period. There was an increase in the volume and value of payment card transactions, the number of cashless transactions, the number of active cards, and the payment terminal network. The share of cashless transactions approached near-total dominance in terms of transaction volume. Consequently, the financial and credit system increasingly operates through remote and cashless channels, heightening the importance of payment security as a component of its stable functioning.

Regarding the second objective, divergent trends were identified concerning the frequency and financial consequences of payment fraud. After peaking, the number of successful fraudulent transactions began to decline; however, the aggregate loss amount and the average loss per successful transaction continued to rise. Simultaneously, the role of social engineering intensified significantly. Thus, the primary shift in the risk profile lies in the transition from the dominance of transaction volume to the growing significance of financial severity and behavioral mechanisms.

Regarding the third objective, additive LMDI decomposition enabled the quantification of the drivers behind changes in aggregate financial losses. During 2022–2023, the increase in losses was driven by the combined impact of transaction frequency and average loss magnitude. Over the subsequent two-year intervals, the situation changed fundamentally. The frequency effect turned negative, partially curbing the rise in losses, whereas the average severity effect became the decisive factor in the further worsening of financial outcomes associated with fraud. Consequently, the LMDI decomposition confirmed that the rise in losses during the later period was driven not by a higher number of successful fraud cases, but by their increased financial value. Regarding the fourth objective, the normalization of metrics concerning payment exposure confirmed the findings of the absolute analysis. The number of fraudulent transactions per million debit transactions gradually declined, whereas losses per UAH million of payment turnover increased. Thus, the financial and credit system exhibits a simultaneous decrease in the relative frequency of successful fraud and an increase in its financial severity. For this reason, assessing the effectiveness of fraud countermeasures based solely on the number of recorded incidents is insufficient.

Regarding the fifth objective, it was determined that the criminal-law significance of the identified trends depends on the actual mechanism by which the act is committed. The growing role of social engineering heightens the importance of deception and abuse of trust, whereas the illicit use of payment details, interference with information systems, dissemination of protected data, or the subsequent concealment of the origin of funds may give rise to different avenues of legal assessment.

The prospects for further research are associated with a more detailed assessment of the transformation of payment-fraud risks using transaction-level and institution-level data. Particular attention should be paid to identifying the relationship

DOI: 10.55643/fcaptp.5.70.2026.5338

between specific fraud mechanisms, the financial severity of losses, customer authorisation patterns, and the effectiveness of preventive measures applied by banks and payment service providers.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Andriushchenko, I. S., & Skydan, V. L. (2023). Digital transformation of the banking sector in Ukraine. *Business Inform, 12*, 77–82. https://doi.org/10.32983/2222-4459-2023-12-77-82
2. Ang, B. W. (2015). LMDI decomposition approach: A guide for implementation. *Energy Policy, 86*, 233–238. https://doi.org/10.1016/j.enpol.2015.07.007
3. Artemieva, I., & Zaliubovska, S. (2023). Digital transformations in the bank sector. *Scientific Bulletin of the National Academy of Statistics, Accounting and Audit*, (1–2), 96–103. https://doi.org/10.31767/nasoa.1-2-2023.10
4. Bondaruk, T. G., Bohrinovtseva, L. M., & Bondaruk, O. S. (2023). Fraud using bank payment cards: A way for financing of terrorism and separatism. *Statistics of Ukraine, 101*(2), 4–13. https://doi.org/10.31767/su.2(101)2023.02.01
5. Boot, A. W. A., Hoffmann, P., Laeven, L., & Ratnovski, L. (2021). Fintech: What's old, what's new? *Journal of Financial Stability, 53*, Article 100836. https://doi.org/10.1016/j.jfs.2020.100836
6. Demchyshak, N., Loik, R., & Loik, A. (2024). Development of digital technologies in the banking system of Ukraine: Innovations in lending, risks and prospects. *Economy and Society*, (61). https://doi.org/10.32782/2524-0072/2024-61-2
7. Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766
8. Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics, 87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x
9. Hordei, O., & Sereda, Ye. (2024). The use of Open Banking in the banking system of Ukraine: Opportunities and risks. *Entrepreneurship and Innovation, 31*, 18–24. https://doi.org/10.32782/2415-3583/31.3
10. Hrechka, V., Ostrovskyi, V., & Bilyi, M. (2025). Development of the financial security system of banking institutions under digitalization. *Scientific Bulletin of Polissia, 2*(29), 461–478. https://doi.org/10.25140/2410-9576-2024-2(29)-461-478
11. Ivashova, L., Larin, S., Shevchenko, N., Antonova, L., Yurchenko, S., & Kryshtanovych, M. (2022). Introduction of Smart-Management into the system of public management of regional development in the context of strengthening national security of Ukraine. *International Journal of Computer Science and Network Security, 22*(9), 369–375. https://doi.org/10.22937/IJCSNS.2022.22.9.49
12. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019
13. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber risk, market failures, and financial stability* (IMF Working Paper No. 17/185). International Monetary Fund. https://doi.org/10.5089/9781484313787.001
14. Kryshtanovych, M., Koval, O., Chernov, S., Bardadym, M., & Kovalenko, L. (2023). The impact of the war on the economic and legal environment of the regions in terms of ensuring national security. *Cuestiones Políticas, 41*(77), 172–183. https://doi.org/10.46398/cuestpol.4177.12
15. Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*, 289–375. https://doi.org/10.1086/501508
16. Liubkina, O., & Taraba, V. (2025). Payment system of Ukraine: Analysis and dynamics of fraudulent transactions. *Economy and Society*, (71). https://doi.org/10.32782/2524-0072/2025-71-165
17. Shapoval, R. V., Orlovskyi, R., Sykal, M., & Zlyvko, S. (2021). Counteraction to offenses committed with the use of electronic payment systems: New challenges and problems. *Amazonia Investiga, 10*(44), 261–269. https://doi.org/10.34069/AI/2021.44.08.25

18. Sharenko, M. S., & Dobrunova, K. V. (2025). Open Banking in Ukraine: Development potential and benefits for consumers. *Analytical and Comparative Jurisprudence*, (1). https://doi.org/10.24144/2788-6018.2025.01.92

19. Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation, 41*, Article 100833. https://doi.org/10.1016/j.jfi.2019.100833

20. Usmanov, R. A. (2024). Some issues of the objective aspect of fraud committed through illegal operations using electronic computing equipment. *Law Journal of Vasyl' Stus Donetsk National University, 1*, 223–229. https://doi.org/10.31558/2786-5835.2024.1.22

21. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

22. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674. https://doi.org/10.1002/asi.20779

Парасюк Н., Лісіцина Ю., Романцова С., Дільна З., Серкевич І.

ФІНАНСОВО-КРЕДИТНА СИСТЕМА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА КРИМІНАЛЬНО-ПРАВОВІ РИЗИКИ ПЛАТІЖНОГО ШАХРАЙСТВА

Фінансово-кредитна система в умовах цифрової трансформації характеризується стрімким розширенням безготівкових платежів, дистанційного банкінгу та нових способів взаємодії між фінансовими установами й клієнтами. Разом із цим змінюється характер ризиків платіжного шахрайства, оскільки зниження відносної частоти незаконних операцій може супроводжуватися збільшенням фінансової тяжкості окремих випадків і поширенням соціальної інженерії. Метою дослідження є оцінювання трансформації ризиків платіжного шахрайства у фінансово-кредитній системі та визначення кримінально-правового значення виявлених змін за умов посилення ролі дистанційних фінансових послуг. Інформаційну базу сформовано з офіційних даних Національного банку України, Департаменту кіберполіції Національної поліції України та положень кримінального законодавства. Методичний підхід поєднує оцінювання динаміки платіжної активності, адитивну LMDI-декомпозицію фінансових втрат на ефект частоти й ефект середньої тяжкості, нормування показників відносно обсягу платіжних операцій, структурний аналіз ролі соціальної інженерії та кримінально-правову систематизацію основних каналів ризику. Результати засвідчили, що розширення платіжної активності супроводжується зниженням відносної частоти успішних шахрайських операцій, однак фінансова тяжкість таких випадків зростає. Одночасно посилюється роль соціальної інженерії, що зміщує акцент із суто технічного захисту платіжної інфраструктури на захист поведінкового процесу прийняття рішення користувачем. Наукова новизна полягає в адаптації LMDI-декомпозиції до оцінювання платіжного шахрайства та її поєднанні з нормованими показниками платіжної експозиції й кримінально-правовою інтерпретацією. Практична цінність результатів полягає в можливості використання запропонованого підходу банками, регулятором і правоохоронними органами для одночасного оцінювання інтенсивності шахрайства, фінансової тяжкості, поведінкових механізмів і потенційно релевантних напрямів правового реагування.

Ключові слова: фінансово-кредитна система, цифрова трансформація, платіжні картки, платіжне шахрайство, кіберризик, соціальна інженерія, кримінально-правовий захист, LMDI-декомпозиція, безготівкові платежі

JEL Класифікація: G21, G23, G28, K42, O33, C43

DOI: 10.55643/fcaptp.5.70.2026.5338