DOI: 10.55643/ser.4.54.2024.582

DESCRIPTION OF NEW FINANCIAL FRAUD AND MONEY LAUNDERING SCHEMES DURING THE WAR IN UKRAINE

Vitaliia Koibichuk
Candidate of Economy Sciences, Associate Professor of the Department of Economic Cybernetics, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-3540-7922

Valeriia Kochnieva
Student of the Department of Economic Cybernetics, Sumy State University, Sumy, Ukraine;
email: v.kochnieva@student.sumdu.edu.ua
ORCID: 0009-0007-2600-8907
(Corresponding author)

Anna Buriak
PhD in Economics, Associate Professor of the Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0003-2954-483X

Yaroslav Petrushenko
PhD Student of the Department of International Economic Relations, Sumy State University, Sumy, Ukraine;
ORCID: 0009-0000-4972-8631

Yuliia Yehorova
PhD in Economics, Associate Professor of the Research Institute of Trade and Sustainable Business, University of Economics in Bratislava, Bratislava, Slovakia;
ORCID: 0000-0002-8756-4073

Received: 13/09/2024
Accepted: 26/12/2024
Published: 31/12/2024

ABSTRACT

This article explores the emergence and evolution of financial fraud and money laundering schemes in Ukraine during the war. The study uses qualitative analysis methods, including a systematic review of news reports, scientific papers, and publicly available data. The findings reveal significant growth in financial fraud activities following the start of the full-scale invasion of Ukraine, driven by economic instability, emotional vulnerability, and trust in charitable initiatives. Key fraudulent schemes are categorized and analyzed, including volunteer fraud, fake investment projects, charity fraud, sales fraud, and banking and card scams. Furthermore, the study examines new fraudulent tactics, such as targeting government aid programs, impersonating social service representatives, and exploiting the psychological distress of victims. The research highlights how fraudsters quickly adapt to new circumstances during the war, creating increasingly sophisticated schemes to fraud individuals, military personnel, and organizations. Practical recommendations are provided for the prevention, detection, and mitigation of financial fraud in war contexts. These include enhancing public awareness, strengthening cybersecurity measures, improving legal frameworks, and fostering international cooperation to address the transnational nature of financial crimes. The study underscores the need for coordinated efforts between governmental structures, law enforcement agencies, and financial institutions to combat the rapidly evolving threat of financial fraud and money laundering during the war.

Keywords: financial fraud, money laundering, war, fraud, cybersecurity, full-scale invasion, Ukraine

JEL Classification: K40, K42

INTRODUCTION

The rapid technological transformation and development of the digital economy and finances have significantly simplified and accelerated the functioning processes of both global and national economic systems. These advancements, while beneficial, have also laid the ground for the rise of cybercriminal activities, particularly financial crimes. With the spread of online banking, digital payment cards, and other online financial services, committing financial fraud has become increasingly easier. This paper explores the worldwide problem of increasing financial fraud, highlighting the greater risks during the war in Ukraine. Economic instability, changes in government priorities, and weakened public morale during conflicts create ideal conditions for fraudsters and organized criminal groups to manipulate financial flows and launder money through international channels.

The urgency of addressing financial fraud is highlighted by recent statistics, which reveal that in 2024, scammers globally stole over USD 1.03 trillion, according to the Global Anti-Scam Alliance (2024). During the war, this problem worsens as conflicts, sanctions, and political instability provide many opportunities for financial fraud. This paper aims to identify and understand the main areas of fraudsters' activities, the vulnerabilities they exploit, and their action patterns. It provides detailed insights into the rise of financial fraud during the war, highlighting how these conditions worsen the problem and exploring ways to reduce the risks.

By exploring these factors, the paper seeks to provide a comprehensive understanding of financial fraud's dynamics in the context of war in Ukraine. It emphasizes the importance of identifying the vulnerabilities within financial systems and the patterns of fraudulent activities to develop effective strategies for prevention and mitigation of them. This understanding is crucial for safeguarding the financial integrity of both national and global economic systems, particularly during periods of heightened instability and conflict.

LITERATURE REVIEW

Given the increased interest of scientists in studying financial fraud, especially in the context of war, the latest scientific publications and research papers devoted to investigating financial fraud in the context of the war in Ukraine were analyzed.

Numerous publications by Ukrainian scientists are devoted to studying various aspects of financial crime during the war in Ukraine. For instance, I. Honcharenko (2023), in her scientific paper, investigates cyber threats to the financial sector during the war. The scientist investigates and lists the following most common cyber threats to the financial sector: phishing, malware distribution, DDoS attacks, credit card fraud, and others. In addition, she offers the following most effective methods for detecting cyber threats in the financial sector: network monitoring, behaviour analysis, event log management, regular penetration testing, and artificial intelligence.

Y. Reshetnyak (2023) studies the issue of formalization and typology of financial fraud in the context of war. He provides a full analysis of various approaches to grouping financial fraud by scientists from different regions. Also, scientists analyze financial fraud types during the war in Ukraine.

T. Bondaruk, L. Bohrintseva, and O. Bondaruk (2023 b), in their scientific work, examine in more detail fraud using bank payment cards as a way of financing terrorism and separatism, and they emphasize the need to strengthen control over financial transactions, particularly through the improvement of identification systems and transactions monitoring.

T. Klyoba and L. Klyoba (2022) in their research examine cyber-attacks on Ukraine's banking sector during the war, highlighting global trends such as phishing, DDoS attacks, and malware. It identifies specific threats like Deepfakes, Zero Trust, and SQL injections while analyzing Ukraine's legislative response and the banking system's adaptability. Scientists give recommendations to mitigate risks, which include updating protective software, vulnerability scanning, penetration tests, and using game theory for scenario planning.

Cybersecurity challenges facing Ukraine's financial sector during the full-scale invasion, analyzing trends, methods, and tools of modern cyber fraud is part of the scientific research paper made by S. Yehorycheva, A. Hlushko, and Y. Khudolii (2023). The authors identify threats, evaluate countermeasures, and provide recommendations to enhance information security, including stricter access controls, personnel behaviour algorithms, and digital security practices. The research emphasizes the importance of aligning with international information security principles and Ukrainian legislation to mitigate cyber risks.

Y. Romanovska, G. Kozachenko, Y. Pogorelov, O. Pomazun, K. Redko (2022) in their work analyze the prospects for stable economic development and economic security during war in Ukraine. Scientists also identify major threats and challenges to Ukraine's economic security, identifying key factors like military destruction by the Russian regime, COVID-19's impact on business activity, budget deficit, and corruption. They highlight the need to modernize outdated production bases, update the legislative framework, and address environmental and demographic issues.

Among the community of foreign scientists, the topic of financial fraud during the war in Ukraine is also a fairly common topic for research. The problem of a sharp increase in corruption during the war in Ukraine was studied by the scientist J. Cifuentes-Faura (2024). In his paper, scientists examine corruption in Ukraine during the full-scale invasion, focusing on political and bureaucratic corruption. J. Cifuentes-Faura highlights cases of embezzlement, bribery, and abuse of power detected during the war in Ukraine. The author analyzes Ukraine’s Corruption Perception Index, noting slight improvements, and proposes a 10-point anti-corruption plan. In another scientist’s paper (Cifuentes-Faura, 2023), he examines the role of accounting in disaster mitigation and emphasizes the importance of transparency in preventing corruption.

Despite active research into the topic of financial crimes and fraud during the war in Ukraine by both Ukrainian and foreign scientists, the issue of specifying the description and determination of areas of financial fraud and descriptions of specific fraudulent schemes remains insufficiently researched.

DOI: 10.55643/ser.4.54.2024.582

AIMS AND OBJECTIVES

The aim of this study is to identify new trends in financial fraud during the war in Ukraine and describe new financial fraud schemes thar were created and developed during the full-scale invasion of Ukraine. In addition, the aim of this study is to provide practical recommendations for both the population of Ukraine and the authorities on how to prevent financial fraud.

The tasks of this paper are:

- to identify the main trends in financial fraud during a full-scale invasion of Ukraine;
- within the framework of identified trends, identify and describe new financial fraud schemes;
- to make recommendations for both the population and the authorities of Ukraine on how to prevent financial fraud.

METHODS

For this research, a number of scientific methods and approaches were used to get desirable results – identify and describe new financial fraud schemes in Ukraine during the war. A comprehensive analysis of literature, scientific works, and reports was conducted to understand the current state of financial fraud and money laundering during the war and to find the main research subtopics and directions. Moreover, news publications and other media publications were analyzed. It is also important to mention methods like synthesis, inductive and deductive analysis, and critical analysis that were used to make a new view of the topic.

RESULTS

In October 2023, the National Bank of Ukraine (NBU) published the results of a survey conducted with the company Opendatabot (National Bank of Ukraine, 2023). The survey involved 112.9 thousand respondents and revealed that 11% of respondents (one to nine people) had been victims of fraud since the start of the full-scale invasion in Ukraine. Additionally, the survey showed that the most common victims were the young part of the population (18 – 24 years old, 14% of respondents) and individuals over 65 years old (11.5% of respondents). The majority of frauds occurred during online buying or selling transactions (52.7%), followed by phishing scams (18.6%) and social media account hacks (12%).

According to the reports from the Prosecutor General's Office of Ukraine, the number of registered fraud cases in 2023 reached a record number for the period 2013 – 2023, with 82 609 registered cases, which is 2.6 times more than the number of registered frauds in 2022 and 2021 (Prosecutor General's Office of Ukraine, 2023) (Figure 1).

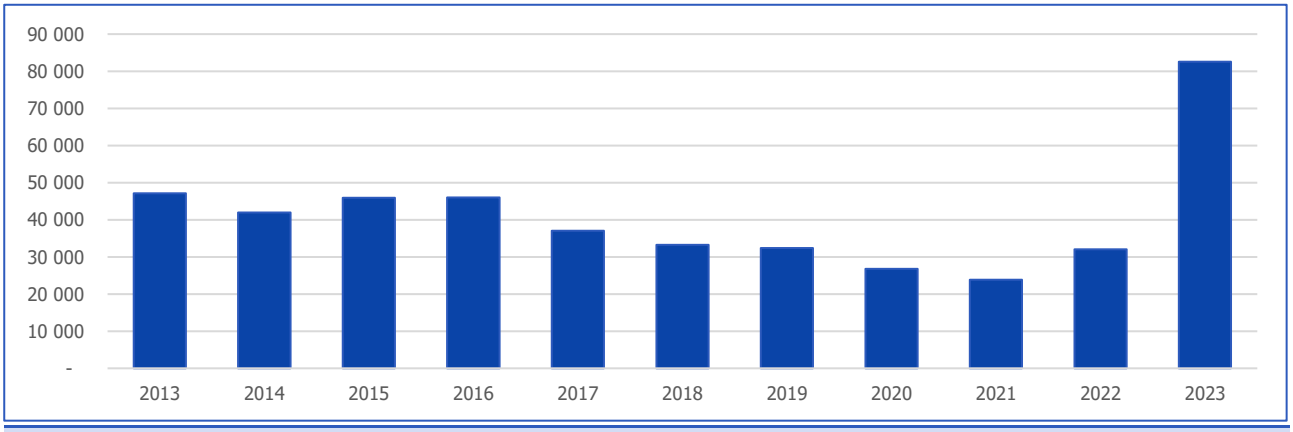

Figure 1. Number of registered fraud cases.

Figure 1 shows that fraud activity rose sharply after the start of the full-scale invasion of Ukraine in 2022. According to Minfin, the following factors are noted as reasons for the increase in fraud during the war (Minfin, 2023):

- the concentration of government attention on supporting military needs, which can cause complications in other sectors;

- an increase in public trust toward charitable organizations, particularly volunteer initiatives, as well as private fund-raising;
- a significant number of the population losing their sources of income, property, and housing, which limits their ability to earn legal income;
- urgent needs that make people willing to pay any price, even to unknown or unverified individuals.

The problem of a significant rise in financial fraud and the increased activity of fraudsters is evident on a global scale. In the report "Interpol Global Financial Fraud Assessment" (2024), Interpol highlights that financial fraud has not only grown but also become more varied, both in the types of crimes committed and the methods used.

While there is generally no clear classification of fraudulent schemes that were created and developed during the war, analyzing the actions of fraudsters shows that there are a number of similar patterns in committed financial frauds. Table 1 represents a categorization of fraudulent schemes that appeared during the full-scale invasion of Ukraine, based on data from the Ministry of Finance of Ukraine (Minfin, 2023).

Table 1. Categorization of Financial Fraud Schemes during full-scale invasion in Ukraine.

Fraud Category	Types of Frauds
Volunteer Fraud	▪ Searching for information on missing persons. ▪ Fake evacuation schemes.
Investment Fraud	▪ Fake investment projects.
Charity Fraud	▪ Fake fundraising for the military needs. ▪ Sale of humanitarian aid.
Sales Fraud	▪ Sale of counterfeit goods. ▪ Real estate fraud.
Banking and Card Fraud	▪ Card frauds. ▪ Fraud related to insurance payments.

As mentioned earlier, financial frauds during the war are not limited to a specific classification. A key feature of fraudsters during the war is their ability to adapt to new circumstances. After the beginning of the full-scale invasion, special programs for disbursing funds to the Ukrainians emerged, such as eSupport, financial aid for war victims, and UN payouts. The rise in the number of such programs has also led to an increase in financial frauds connected to them. For instance, in 2024, a new fraud scheme related to the "Winter eSupport" payment program was detected. The Ministry of Social Policy warned Ukrainians about fake messages supposedly sent from the Ministry itself. The fraudulent scheme involves links shared on platforms, like Telegram, that direct users to a fraudulent website asking for personal and credit card information, allowing fraudsters to access money from a stolen bank account (Ministry of Social Policy of Ukraine, 2024, Hromadske 2024). Given the financial difficulties faced by many Ukrainians during the war, the first victims of such fraudulent schemes have already been detected. For instance, in December 2024, a 49-year-old woman from the Chernivtsi region, Ukraine, lost nearly UAH 100.000, becoming a victim of fraudsters who promised her to pay money from the "Winter eSupport" program made by President Zelensky. The woman told the police that she saw an announcement in one of the messengers about the possibility of receiving payments. After clicking on the link and registering with her confidential credit card information, UAH 98.960 was withdrawn from her bank account (TSN, 2024). A similar situation happened with a 38-year-old resident of the Khmelnytskyi region in Ukraine. After clicking on the link, the man entered his personal data and, after receiving a message with a confirmation code UAH 25.000, disappeared from his bank account (XM – INSIDE).

One of the key characteristics of financial fraud during the war is the fact that it involves emotional manipulation. The war significantly impacts the psychological state of the population, creating feelings of anxiety, fear, uncertainty, and vulnerability. Fraudsters expertly exploit these emotions, creating situations that make people act impulsively. One such type of financial fraud involves an offer to release prisoners of war or help to find the body of a fallen soldier for a sum of money to their relatives. Fraudsters exploit the emotional vulnerability of relatives and friends in such situations, and after receiving payment, they disappear. A real example of this fraudulent scheme occurred on February 20, 2023, when the Security Service of Ukraine arrested men in Kyiv who had extorted USD 60 000 from the relatives of two Ukrainian prisoners of war, promising to exchange money with Russian soldiers for their inclusion in the "exchange lists" (UNIAN News 2023).

DOI: 10.55643/ser.4.54.2024.582

Fraud targeting vulnerable groups of the population – pensioners and single people, is particularly common during the war. Fraudsters most often defraud pensioners, posing as social workers or representatives of charitable foundations and organizations. The Main Department of the National Police in Kyiv draws attention to the intensification of such financial fraud schemes, especially during the war. The main scheme of action of fraudsters is similar. The head of the Shevchenkivskyi Police Department, Ihor Padiuk, notes (The Main Department of the National Police in Kyiv, 2023): "Criminals enter the homes of unsuspecting citizens under the pretext of exchanging money, assigning a non-existent pension supplement, providing material or other assistance, or offering to purchase food at low prices." The trend of spreading fraud targeting vulnerable groups of the population is also spreading to other regions of Ukraine. The most popular scheme by which fraudsters defraud pensioners is the scheme called "your relative is in trouble." Given the scale of such schemes, it is worth paying attention to specific examples of exploiting the trust of vulnerable parts of the population. The events covered in the news not only confirm the seriousness of the problem but also allow us to understand the characteristic features and mechanisms of the attackers' work. Here are a few examples that reveal the essence of financial fraud aimed at vulnerable segments of the population, especially in times of war:

- in Ternopil, fraudsters deceived a pensioner out of more than UAH 50.000 by calling her, pretending to be her granddaughter and claiming she had been hospitalized (Suspilne Kyiv, 2023);
- in Chernihiv, a fraudster scammed an 84-year-old pensioner out of UAH 60.000 by calling and pretending to be her sister, asking for financial help for medical treatment after a non-existent car accident (Suspilne Chernihiv, 2024).

Another emerging type of fraud targeting internally displaced persons (IDPs) is reported by the Pension Fund of Ukraine. Fraudsters, posing as Pension Fund employees, ask IDPs undergoing physical identification to provide their bank card details. The Pension Fund clarifies that it never requires card details for identification or payment processes (Pension Fund of Ukraine, 2024). Another growing fraud involves fake SMS messages from postal services, claiming that packages can't be delivered due to missing addresses. The links in these messages lead to phishing websites designed to steal sensitive data and funds from bank accounts.

In December 2024, a new fraud targeting entrepreneurs was reported. Criminals, posing as representatives of the Kyiv Regional Military Administration, ask for financial help for the military (Suspilne Kyiv, 2024). However, the administration clarified it never solicits such donations, as all charitable contributions are made through proper channels. A similar situation was recorded in Sumy. Several businesses have reported receiving letters allegedly from the Head of the Sumy Regional Military Administration, requesting financial contributions to support the military. The Sumy Regional Military Administration has officially stated that these requests are part of a fraudulent scheme (Sumy Today, 2024).

Fraud targeting military personnel has become increasingly prevalent since the full-scale invasion began. These scams have risen in number and spread widely. For instance, fraudsters have been posing as government officials or military representatives, claiming to offer assistance, seek donations, or promise benefits. These tactics exploit the vulnerability and urgency surrounding military service, making service members prime targets for scams.

Since the full-scale invasion, fraud targeting military personnel has sharply increased. Examples include:

- in Kyiv, in August 2024, a prison inmate impersonated a bank employee to steal a soldier's funds by obtaining card details (Suspilne Kyiv, 2024);
- in Rivne, a man from Zaporizhzhia, in collaboration with others, swindled UAH 500.000 from a soldier's account through a mobile scam (Suspilne Zaporizhzhia, 2024);
- a Kyiv-based fraudster deceived 19 military personnel and their families, stealing UAH 600.000 by selling fake military goods online and posing as a soldier (Suspilne Kyiv, 2024);
- a 26-year-old woman from Chervonograd, Lviv region, was being tried for stealing over UAH 350.000 from soldiers and others by selling non-existent military products online by creating pages and social media and receiving payments (Suspilne Lviv, 2024).

During the war, the number of fundraising efforts for the army, citizens affected by the conflict, and humanitarian initiatives has increased significantly. This creates opportunities for fraud, with criminals exploiting the trust in charitable causes to create fake fundraisers via social media, messaging apps, or fake websites. These schemes can lead to big financial losses and damage public trust in volunteer and charitable organizations. Since the full-scale invasion, there has been a notable rise in such fraudulent activities, as shown by the following examples:

- in June 2023, a fraudster in Volyn was arrested for posting fake fundraising messages on Facebook for the treatment of sick children and injured soldiers. Using emotional manipulation, they created 21 fake accounts and collected UAH 250.000 (Suspilne Lutsk, 2023);

- in July 2023, a group of fraudsters in Lviv was exposed for scamming citizens by pretending to organize charitable collections for military personnel's medical treatment (National Police of Ukraine, 2023).

It is impossible not to mention the intensification of money laundering during the war. Unfortunately, some government officials are trying to enrich themselves at the expense of war and use money laundering for that. For instance, in February 2024, a woman who works for authorities is suspected of embezzling 5 million from bomb shelters for children at school. Law enforcement officers established that in 2023, the education department of one of the city councils of the region held a tender for the purchase of modular shelters for schools. Contracts for their supply were concluded with the winning company, the only participant in the competition. However, the cost of the shelters supplied is significantly higher than the market price, they do not meet the established requirements and were delivered incompletely. The woman involved an acquaintance in the criminal scheme. He found a controlled LLC, which the suspect ensured victory in the tender (Ukrainian Pravda, 2024). In another suspicious case, the Kyiv Education Department of the Dnipro district purchased over 300 drums for nearly UAH 900.000, citing their use for children's psychological relief during air raids in shelters. While the purchase was officially for kindergartens, the drums' deployment in shelters raised concerns about the true purpose of the funds. The significant expenditure of non-essential items during the war, coupled with questions over how the drums ended up in shelters, has prompted investigations into potential misallocation or misuse of public funds, raising red flags for possible money laundering (Suspilne Kyiv, 2023).

Due to the urgency of the issue of combating financial fraud and money laundering in Ukraine, especially during the war, it is important to continue reforming the financial system and improving national monitoring mechanisms. Thus, on October 17 and 18, 2023, the First Deputy Minister of Finance of Ukraine, Denys Ulyutin, became the speaker of two events dedicated to discussing ways to improve the financial monitoring system in the country and countering the laundering of funds obtained illegally. In his speeches, he emphasized that, despite the challenges of a full-scale war, Ukraine continues to strengthen the legislative framework for combating money laundering and terrorist financing. In particular, it was noted that draft law No. 10072 was adopted, which harmonizes Ukrainian legislation with international standards, in particular the recommendations of the Financial Action Task Force (FATF).

In particular, the FATF – Financial Action Task Force, in its report "The FATF Recommendations", offers to countries several measures to combat money laundering:

1. Risk assessment and the application of a risk-based approach.
    - Countries should identify, analyze, and understand the risks associated with money laundering and terrorist financing.
    - It is necessary to appoint an authorized body or introduce a mechanism to coordinate the assessment of risks and effectively reduce them.
    - Based on these assessments, a risk-based approach should be implemented, ensuring that measures correspond to the identified threats.
    - In areas with a high level of risk, enhanced control measures should be applied, while simplified procedures can be implemented for areas with a low level of risk.
    - It is also necessary to identify and analyze the risks associated with financing the proliferation of weapons of mass destruction and take measures to minimize them.
    - Financial institutions and other designated non-financial entities should independently assess risks and apply effective measures to mitigate them.
2. National cooperation and coordination.
    - Develop national policies based on identified risks, regularly update them, and designate bodies or mechanisms for implementation.
    - Ensure effective mechanisms for cooperation and information exchange between policymakers, financial intelligence, law enforcement, supervisory authorities, and other relevant structures.
    - Ensure consistency of national requirements with international standards for the protection of personal data, confidentiality, and information security.

DOI: 10.55643/ser.4.54.2024.582

DISCUSSION

The results of the study highlight the alarming increase in financial fraud in Ukraine during the period of full-scale invasion. Notably, the survey conducted by the National Bank of Ukraine (NBU) and Opendatabot indicates that 11% of respondents had been victims of fraud, with young adults (18–24 years old) and individuals over 65 years old identified as the most common victims. This aligns with previous research highlighting the vulnerability of specific age groups to fraud, particularly during crises. Similarly, the sharp rise in registered fraud cases reported by the Prosecutor General's Office emphasizes the severity of the issue, with 82 609 cases in 2023, a 2.6 increase compared to prior years. These findings support trends observed globally, as noted in the Interpol Global Financial Fraud Assessment (2024), which underscores the expansion and diversification of fraudulent schemes worldwide. The categorization of fraudulent schemes further highlights the adaptability and innovation of fraudsters during the war.

One of the most significant findings is the extent to which fraudsters target vulnerable populations, including pensioners and internally displaced persons (IDPs). The examples from different cities in Ukraine, where fraudsters posed as relatives or officials to deceive pensioners, reflect a high level of exploiting trust and emotional vulnerability. Such cases resonate with prior studies indicating that older adults are particularly susceptible to such scams. Similarly, fraud targeting military personnel and fundraising initiatives highlights the exploitation of national and communal solidarity during the war. The examples provided demonstrate the fraudsters' ability to undermine trust in charitable organizations and institutions.

The findings highlight the increase in money laundering, exemplified by the embezzlement of funds meant for school shelters. This issue aligns with global concerns about money laundering during crises, as noted in FATF's recommendations. Efforts to align Ukrainian law with international standards, like draft law No. 10072, show a proactive approach, though challenges persist.

This study has several limitations. Firstly, while the data from surveys and government reports provide valuable insights, the reliance on secondary data may not capture the full extent of fraud activities, particularly unreported cases. Second, the categorization of fraudulent schemes is based on available data, which may not encompass emerging or less-documented forms of fraud.

CONCLUSIONS

In conclusion, this study has explored the significant rise of financial fraud in Ukraine during the full-scale invasion, revealing significant trends and innovative schemes developed by fraudsters. A number of factors have led to an increase in fraudulent activity, including the concentration of government attention on supporting military needs, an increase in public trust toward charitable organizations, and financial and psychological difficulties of Ukrainians.

The analysis of financial fraud during the full-scale invasion of Ukraine highlights several critical trends. Fraud cases have surged to the highest level, with online scams such as phishing and social media account hacks being the most prevalent. Vulnerable groups, including pensioners, internally displaced persons and military personnel, have become primary targets due to emotional manipulation and impersonation schemes. Fraudsters have also exploited public trust in government assistance programs and charitable initiatives, leading to widespread misuse of funds and loss of trust. Additionally, war conditions have facilitated complex money-laundering schemes involving public officials.

In response to these challenges, the Financial Action Rask Force (FATF) has provided recommendations to enhance fraud prevention and combat money laundering. Key measures include conducting risk assessments, implementing risk-based approaches, strengthening national cooperation and coordination, and ensuring alignment with international standards.

Future research should focus on developing effective countermeasures specifically designed for wartime conditions, such as enhanced public awareness campaigns, improved legislative frameworks, and technological solutions for fraud prevention.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

This article was prepared as part of a research projects 0123U101945 and 0124U000544.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Rogers, S. (2024, November 7). *International Scammers Steal Over $1 Trillion in 12 Months in New Global State of Scams Report*. GASA. https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai
2. Honcharenko, I. (2023). Cyber threats to the financial sector in the context of war. *Economics and Society, 50.* https://doi.org/10.32782/2524-0072/2023-50-82
3. Reshetnyak, Y. (2023). Formalization and typology of financial frauds in the context of military conflict. *Via Economica, 3*, 145–151. https://doi.org/10.32782/2786-8559/2023-3-22
4. Bondaruk, T. G., Bohrinovtseva, L. M., & Bondaruk, O. S. (2023b). 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. Klyoba, L., & Klyoba, T. (2022). CYBER THREATS TO THE BANKING SECTOR UNDER MARTIAL LAW IN UKRAINE. *Financial and Credit Activity: Problems of Theory and Practice, 5*(46), 19–28. https://doi.org/10.55643/fcaptp.5.46.2022.3883
6. Yehorycheva, S., Hlushko, A., & Khudolii, Y. (2023). Issue of Ukrainian financial sector information security. *DEVELOPMENT MANAGEMENT*, *21*(4), 45–52. https://doi.org/10.57111/devt/4.2023.45
7. Romanovska, Y., Kozachenko, G., Pogorelov, Y., Pomazun, O., & Redko, K. (2022). Problems of Economic Security Development in Ukraine: Challenges and Opportunities. *Financial and Credit Activity Problems of Theory and Practice, 5*(46), 249–257. https://doi.org/10.55643/fcaptp.5.46.2022.3906.
8. Cifuentes-Faura, J. (2024). Corruption in Ukraine during the Ukrainian–Russian war: A decalogue of policies to combat it. *Journal of Public Affairs, 24*(1). https://doi.org/10.1002/pa.2905
9. Cifuentes-Faura, J. (2023). Government transparency and corruption in a turbulent setting: The case of foreign aid to Ukraine. *Governance.* https://doi.org/10.1111/gove.12835
10. National Bank of Ukraine. (2023, October 9). Results of a survey by the NBU and Opendatabot: every ninth respondent became a victim of fraudsters since the beginning of martial law. https://bank.gov.ua/ua/news/all/rezultati-opituvannya-vid-nbu-ta-opendatabot-kojen-devyatiy-opitaniy-stavav-jertvoyu-shahrayiv-z-pochatku-voyennogo-stanu
11. General Prosecutor's Office. (n.d.). *On registered criminal offenses and the results of their pre-trial investigation*. Office of the General Prosecutor. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
12. Minfin. (2023, November 2). New types of fraud during the war and how not to fall for the scammers' tricks. Minfin - all about finance: news, exchange rates, banks. https://minfin.com.ua/ua/2023/11/02/115264862/
13. INTERPOL Financial Fraud assessment: A global threat boosted by technology. (2024, March 11). INTERPOL. The International Criminal Police Organization. https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology
14. Ministry of Social Policy of Ukraine (2024). Ministry of Social Policy of Ukraine. https://www.msp.gov.ua/news/24166.html
15. Scammers Distribute Fake Links for 1,000 UAH State Payment — Ministry of Social Policy. (2024). Hromadske. https://hromadske.ua/suspilstvo/233835-shakhrayi-poshyriuiut-feykovi-posylannia-na-vyplatu-1000-hryven-vid-derzavy-minsotspolityky
16. Scammers Defraus Resident of Shepetivka District with "Zelensky Thousand" Scheme for 25,000 UA – XM-INSIDE. XM-INSIDE. https://www.xm-inside.com/news/shahrayi-tysyacheyu-vid-zelenskogo-oshukaly-zhytelya-shepetivshhyny-na-%e2%82%b425-tysyach/
17. Fraudulent Schemes with the "Zelensky Thousand": Woman Loses Nearly 100,000 UAH. TSN.ua (2024, December 11). https://tsn.ua/exclusive/shahrayski-shemi-z-tisyacheyu-zelenskogo-zhinka-vtratila-mayzhe-100-tisyach-griven-2721168.html
18. Easy Money, or How Scammers Profit from Ukrainians During the War. (2023). UNIAN News - Latest News of Ukraine Today. https://www.unian.ua/economics/finance/legki-groshi-abo-yak-shahraji-nazhivayutsya-na-ukrajincyah-pid-chas-viyni-12459213.html
19. Metropolitan law enforcement officers continue to warn citizens about scammers' "traps" (2023). The Main Department of the National Police in Kyiv https://kyiv.npu.gov.ua/news/stolychni-pravookhorontsi-prodovzhuiut-poperedzhaty-hromadian-pro-pastky-shakhraiv

DOI: 10.55643/ser.4.54.2024.582

20. In Ternopil, scammers defrauded a pensioner of over 50 thousand hryvnias (2023). Suspilne Kyiv https://kyiv.npu.gov.ua/news/stolychni-pravookhorontsi-prodovzhuiut-poperedzhaty-hromadian-pro-pastky-shakhraiv.

21. "Sister got into a traffic accident": a man was detained who defrauded a pensioner from Chernihiv of 60 thousand hryvnias (2024). Suspilne Chernihiv https://suspilne.media/chernihiv/853315-sestra-potrapila-v-dtp-zatrimali-colovika-akij-osukav-pensionerku-z-cernigova-na-60-tisac-griven/

22. Pension Fund of Ukraine. (n.d.). *Fraudsters try to deceive pensioners during the identification process*. Pension Fund of Ukraine. https://www.pfu.gov.ua/2163478-shahrayi-namagayutsya-oshukaty-pensioneriv-u-protsesi-identyfikatsiyi/

23. Kyiv Regional Military Administration. (n.d.). Requesting money for the military: The head of the regional military administration warns about fake letters sent to entrepreneurs. Suspilne Kyiv. https://suspilne.media/kyiv/896747-prosat-grosi-dla-vijskovih-ocilnik-ova-zaavlae-so-vid-jogo-imeni-nadsilaut-fejkovi-listi-pidpriemcam/

24. Sumy Today. (2024, December 13). In the Sumy region, fraudsters posing as the Head of the Sumy Regional Military Administration are collecting funds for the military. https://sumy.today/news/politics/44719-na-sumshchyni-shakhrai-prykryvaiuchys-imiam-nachalnyka-sumskoi-ova-zbyraiut-koshty-na-armiiu.html

25. Kyiv Prosecutor's Office. (n.d.). Defrauding a soldier: Kyiv pretrial detention inmate faces trial for fraud. Suspilne Kyiv. https://suspilne.media/kyiv/877533-osukav-vijskovosluzbovca-u-kievi-arestanta-sizo-suditimut-za-sahrajstvo/

26. Kyiv Regional Military Administration. (n.d.). Scamming a serviceman: Kyiv pre-trial detention center inmate to face fraud charges. Suspilne. https://suspilne.media/kyiv/877533-osukav-vijskovosluzbovca-u-kievi-arestanta-sizo-suditimut-za-sahrajstvo/

27. Suspilne Lviv. (2024, December 22). Earned money by selling non-existent drones and ammunition for soldiers: A woman will be tried in Lviv region. Suspilne Media. https://suspilne.media/lviv/662028-zaroblala-na-prodazi-neisnuucih-droniv-ta-amunicii-dla-vijskovih-na-lvivsini-suditimut-zinku/

28. Suspilne. (2023, November 17). Volyn resident who organized fake fundraising for wounded soldiers taken into custody. Suspilne. https://suspilne.media/lutsk/519347-volinanina-akij-organizovuvav-fejkovi-zbori-kostiv-dla-poranenih-bijciv-vzali-pid-vartu/

29. National Police of Ukraine. (2023, November 17). Cyber police in Lviv region uncovered fraudsters who embezzled charitable donations for Ukrainian servicemen in need of medical treatment. National Police of Ukraine. https://www.npu.gov.ua/news/pryvlasniuvaly-blahodiini-vnesky-dlia-viiskovosluzhbovtsiv-zsu-iaki-potrebuiut-dopomohy-na-likuvannia-kiberpolitsiia-lvivshchyny-vykryla-shakhraiv

30. Ukrainian Pravda. (2024, February 7). In the Dnipropetrovsk region, an official is suspected of embezzling 5 million from shelters for schoolchildren. https://www.pravda.com.ua/news/2024/02/7/7440844/

31. Suspilne Kyiv. (2023, June 15). Drums for 900,000 UAH: Musical instruments purchased for shelters in one of Kyiv's districts. Suspilne Media. https://suspilne.media/kyiv/507841-barabani-na-900-tis-grn-v-odnomu-z-rajoniv-kieva-zakupili-muzinstrumenti-dla-ukrittiv/

32. FATF. (2012-2023). International standards on combating money laundering and the financing of terrorism & proliferation. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Койбічук В., Кочнєва В., Буряк А., Петрушенко Я., Єгорова Ю.

ОПИС НОВИХ СХЕМ ФІНАНСОВИХ ШАХРАЙСТВ В УМОВАХ ВОЄННОГО ЧАСУ В УКРАЇНІ

У статті досліджено появу та розвиток нових схем фінансового шахрайства й відмивання грошей в Україні під час війни. Дослідження використовує такі методи аналізу, як систематичний огляд новин, наукової літератури та загальнодоступних даних. Отримані дані свідчать про значне зростання фінансових шахрайств після початку повномасштабного вторгнення в Україні, що пов'язано з економічною нестабільністю, емоційною вразливістю та надмірною довірою до благодійних ініціатив. Ключові шахрайські схеми класифіковані та аналізовані зокрема як волонтерські шахрайства, фейкові інвестиційні проєкти, шахрайства з благодійними організаціями, шахрайства з продажами, а також банківські шахрайства та шахрайства з картками. Крім того, у дослідженні розглянуті нові шахрайські напрями, такі як орієнтація на державні програми підтримки населення, видавання себе за представників соціальних служб і використання психологічного стану жертв. Дослідження підкреслює те, як шахраї швидко пристосовуються до нових обставин воєнного часу, створюючи все більш продумані схеми шахрайств, спрямовані на вразливі категорії населення. Крім того, у статті надано практичні рекомендації щодо запобігання фінансовим шахрайствам, виявлення їх та боротьби з ними в умовах війни. Вони включають підвищення обізнаності громадськості, посилення заходів кібербезпеки, удосконалення законодавчої бази та сприяння міжнародній співпраці для вирішення проблеми глобальності фінансових злочинів. Дослідження підкреслює необхідність об'єднання зусиль державних структур,

правоохоронних органів і фінансових установа для боротьби із загрозою фінансового шахрайства та відмивання грошей.

Ключові слова: фінансові шахрайства, відмивання коштів, війна, шахрайство, кібербезпека, повномасштабне вторгнення, Україна

JEL Класифікація: K40, K42

DOI: 10.55643/ser.4.54.2024.582