CYBER-ENABLED FRAUD AND MONEY LAUNDERING: CURRENT TRENDS AND THREATS

Artur GOLBAN
PhD, CAMS, CGSS, CFCS,
independent AML/compliance expert, Moldova
E-mail: aaartgolb@gmail.com
ORCID: 0000-0001-8188-1011

Abstract: *Cyber-enabled fraud represent illegal activities by which fraudsters use digital tools such as online platforms, internet, e-mail, mobile telephony to obtain sensitive data, money or access to different systems. The money obtained from fraud are laundered via different channels. In this article are analyzed the current trends of cyber-enabled fraud, the ways how the money obtained from fraud are laundered and how to protect the customers in order not to become victims of fraudulent activity. The author analyzes the most frequent types of fraud: phishing, social engineering, card frauds, online transactions frauds, crypto investments scams, online shopping fraud and preventive measures necessary to be applied by financial institutions to protect their customers. In the article are highilighted the role of developing robust internal controls combined with educational programs for customers to prevent cyber enabled frauds.*

Keywords: *Anti-Money Laundering, cyber-enabled fraud, digital world, threats, security.*

Classification JEL: *K42, G18, M42.*

UDC: *343.37:004.056* ***DOI:*** *https://doi.org/10.53486/ser2026.27*

1. Introduction

We live in a world of digitalization. Digitalization contributed substantially to the economic development, but in the same time opened the door to new typologies of fraud, money laundering, financial crimes using advanced technologies.

Cyber-enabled fraud is evolving rapidly being registered more and more victims all around the world. Fraudsters are using automated techniques to commit fraud (bots, deepfake, phishing, etc.)

In this scientific article is analyzed the problem of increasing cyber-enabled frauds and the ways of preventing and combatting them. The main objective of the research is to analyze the current trends of cyber-enabled frauds and threats in order to develop a modern framework of anti-fraud measures and instruments to reduce the risks associated with the digital financial criminality.

The scientific novelty and originality of the scientific paper consists in identification and description of new typologies of fraud in the context of digitalization; presenting new ways of money laundering from cyber enabled fraud; formulating ways of preventing and combatting cyber-enabled frauds.

2. Literature Review

In the academic literature fraud is analyzed very extensively. Exist various researches on fraud from different perspectives: economical, legal, psychological, sociological and technical. The classic literature in the field of fraud (Cressey, 1953; Wells, 2017; Albrecht, 2018) focus more on psychological and organizational mechanisms which generate

fraudulent behavior, being introduced the models such as "fraud triangle"; rationalization theory and occupational frauds.

On the other hand, in modern literature (Goodman, 2015; Holt & Bossler, 2020; Yar, 2020; Casey, 2019; Mitnick, 2002) the analysis of fraud is more and more focused on digital fraud, emphasizind the role of digitalization, globalization and advanced technologies in creation of new typologies, new opportunities of crimes and new detection challenges.

In classic literature the researches were focused mostly on the following typologies of frauds:

- Accounting Fraud;
- Financial Misappropriation;
- Forgery and Deception;
- Occupational and Corporate Fraud.

These frauds are produced mostly manual and local. In modern literature frauds are automated, scalable, cross-border, the researches being focused on the following types of fraud:

- Cyber-enabled fraud;
- Digital identity fraud;
- Crypto / blockchain fraud;
- Phishing, malware, ransomware fraud;
- AI fraud (deepfake, voice cloning);
- FinTech platform fraud.

Goodman, M. (2015) in the book *"Future crimes: Inside the digital underground and the battle for our connected world"* analyzes cyber enabled fraud according to which digital fraud uses technology to deceive. Mitnick, K. D., & Simon, W. L. (2002) in the book *"The art of deception: Controlling the human element of security"* reveals that digital fraud exploits psychological manipulation. Glenny, M. (2011) in the book "DarkMarket: Cyberthieves, cybercops and you" analyzes the online fraud committed in the Internet.

Schneier, B. (2012) in the book "Liars and outliers: Enabling the trust that society needs to thrive" highlights that digital fraud exploits technical vulnerabilities. According to Krebs, B (2014), Holt, T.&Bossler, A. (2020), Yar, M. (2018) and Casey, E. (2019) fraud is using phishing, malware and data theft, where technology plays the central role.

From the literature on fraud which was analyzed we can conclude that nowadays more and more fraudsters activate via digital channels through Internet and technology compared to classic fraud which was more manual and local.

The digitalization of economy created opportunities for the development of cyber-enabled fraud which represent a threat to the financial system stability, business and corporate integrity and individual security, being necessary steps to prevent and combat this increasing phenomenon.

3. Methodology

The scientific investigation is based on the data from the General Police Inspectorate, National Bank of Moldova, INTERPOL, FATF. The analysis covers the period 2023-2025 and focuses on the dynamics of cyber-enabled fraud cases, the value of losses, regional comparisons and the Global Fraud Index.

The research focuses on several key analytical dimensions, including:

- the dynamics of cyber-enabled fraud cases,
- the total and average value of financial losses,
- regional and international comparisons, and
- positioning within the Global Fraud Index, which reflects the relative exposure and vulnerability of countries to fraud-related risks.

To achieve the research objectives, a combination of **quantitative and qualitative methods** has been applied.

Time Series Analysis

The time series method is employed to examine the evolution of cyber-enabled fraud indicators over the 2023–2025 period. This approach allows for the identification of trends, fluctuations, and patterns in the number of reported cases and associated financial losses. Through this method, it becomes possible to detect growth rates, seasonal variations, and potential anomalies, thereby providing a dynamic perspective on the phenomenon under study.

Graphical Method

The graphical method is used to visually represent statistical data through charts, diagrams, and comparative figures. This facilitates a clearer interpretation of complex datasets and enhances the ability to identify relationships between variables such as time, geographical distribution, and financial impact. Visual representations support both descriptive and comparative analysis and contribute to increased transparency of the research findings.

Analysis and Synthesis

The method of analysis involves the decomposition of the studied phenomenon into its constituent elements, such as types of fraud schemes, categories of victims, and channels of execution (e.g., phishing, social engineering, online payment fraud). Conversely, synthesis integrates these elements into a coherent framework, allowing for the formulation of generalized conclusions regarding the structure and mechanisms of cyber-enabled fraud.

Induction and Deduction

Inductive reasoning is applied to derive general conclusions based on empirical observations and statistical data, particularly in identifying emerging trends and risk factors associated with cyber fraud. Deductive reasoning, on the other hand, is used to test existing theoretical assumptions and frameworks against the observed data, ensuring the logical consistency and validity of the findings.

The integration of these methods ensures a multidimensional approach to the study of cyber-enabled fraud. By combining statistical analysis with logical reasoning and visual interpretation,

the research provides both descriptive insights and explanatory value, contributing to a deeper understanding of the phenomenon from both national and global perspectives.

4. Results and Discussion

More frequently people become victims of cyber-enabled fraud, which can be committed by:

- Employees within the organization;
- Management or leadership;
- Customers or suppliers;
- Organized groups or external criminals;
- Corrupt professionals (auditors, accountants, consultants).

According to the 6th Anti-Money Laundering Directive (6AMLD) fraud is one of 22 predicate offences of money laundering (fig.1).

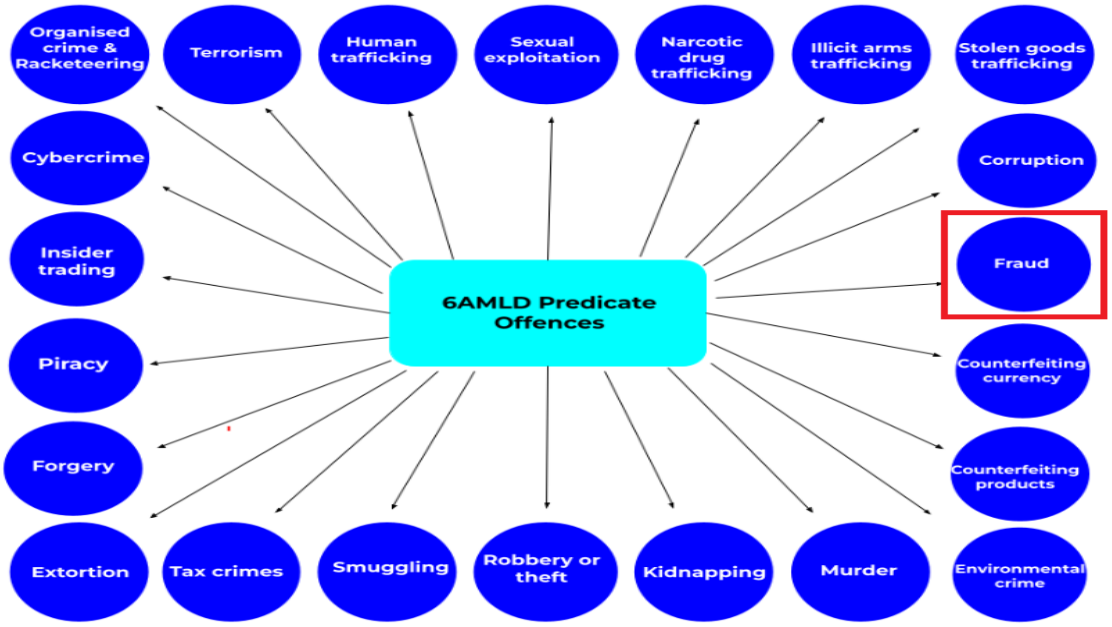


Figure 1. FRAUD – One of the 22 predicate offenses of ML according to 6 AMLD

Source: *https://www.tookitaki.com/compliance-hub/6amld-predicate-offences*

What is behind fraud? The Fraud Triangle

According to Donald R. Cressey, the fraud risk materializes when all 3 elements of fraud (fig.2):

Pressure + Opportunity + Rationalization are combined (1)

Pressure or motivation, as well as rationalization, are rather psychological factors that push the fraudster or create the temptation to commit fraud and the ability to explain to himself that what he is doing is right.

Figure 2. The Fraud Triangle

Source: *https://fitsmallbusiness.com/what-is-the-fraud-triangle/*

Opportunity refers to access to assets or finances, combined with the lack of or weak controls that allow a fraudster to commit fraud and remain undetected.

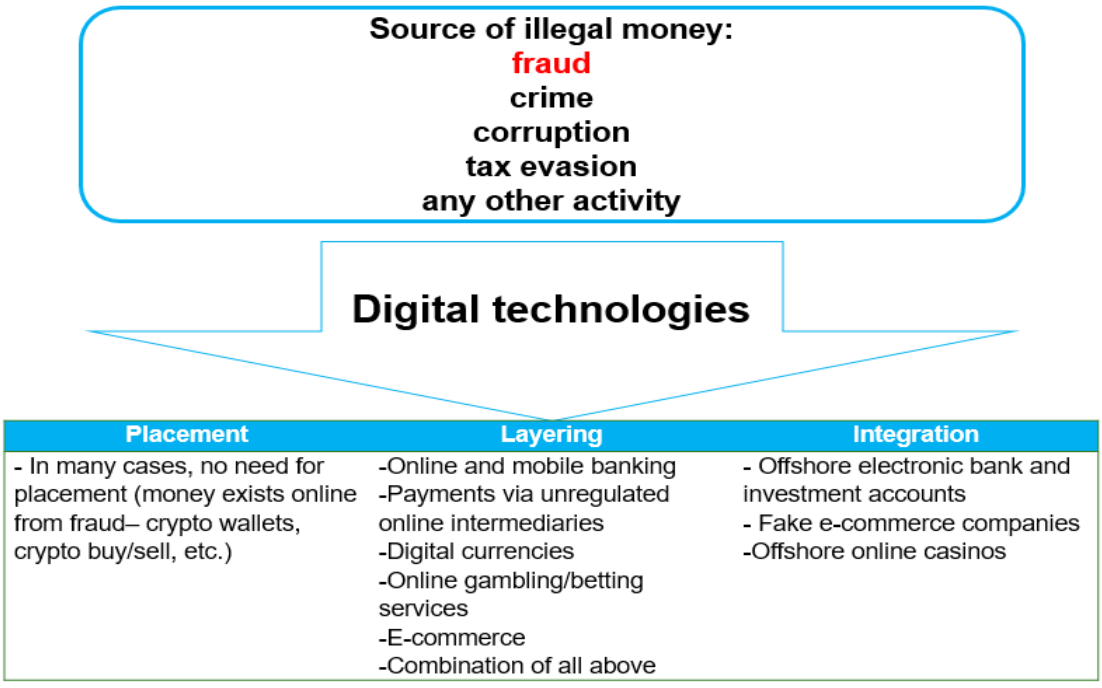


Figure 3. Digital technologies and illegal money transfers

Source: *elaborated by the author*

In fig. 3 is revealed how money from fraud are laundered via digital technologies using 3 stages of money laundering:

1. **Placement** – in many cases, no need for placement, the money exists online from fraud – crypto wallets, crypto buy/sell transactions

2. **Layering** – online and mobile banking, digital currencies, online gambling/betting services, E-commerce, combination of all above
3. **Integration** – offshore electronic bank and investment accounts, fake e-commerce accounts, offshore online casinos, etc.

Figure 4. Financial Fraud among the TOP 5 Global Crime Threats
***Source**: INTERPOL (2026)*

According to INTERPOL (2026) financial fraud is among top 5 global crime threats after: cocaine trafficking, synthetic drugs trafficking, heroin trafficking, money laundering (fig.4).

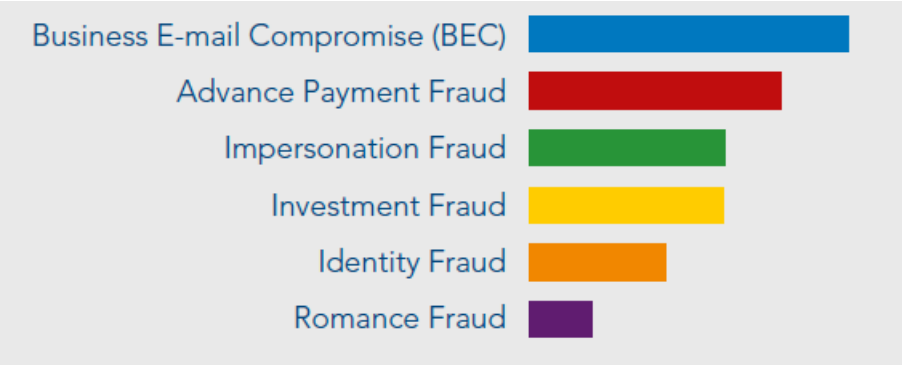


Figure 5. Top Global Financial Fraud Threats Facing Law Enforcement in 2024 and 2025
***Source**: INTERPOL (2026)*

In fig.5 are presented the most frequent financial fraud registered in 2024 and 2025:

1. Business E-mail Compromise (BEC);
2. Advance Payment Fraud;
3. Impersonation Fraud;
4. Investment Fraud;
5. Identity Fraud;
6. Romance Fraud.

According to World Economic Forum (WEF, 2025), more than 77% of business leaders reported an increase of the frauds in 2025.

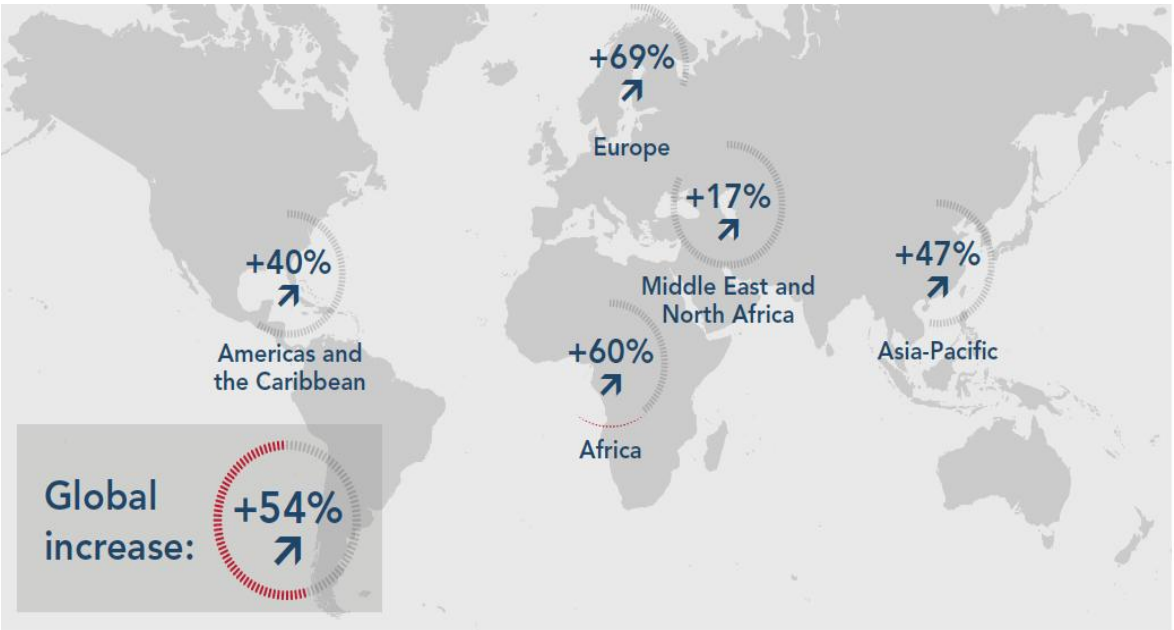


Figure 6. Global increase in financial fraud 2025 vs 2024

***Source**: INTERPOL (2026)*

Analyzing the figure 6 we can reveal that in 2025 was registered a global increase in financial fraud by 54% compared to 2024. In regional context, mostly fraud increased in Europe: + 69%, being followed by Africa:+60%, Asia-Pacific:+47%, Americas ad the Caribbean +40%.

According to the Financial Action Task Force (FATF, 2025) report: "***Cyber-enabled fraud - Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks"*** in 156 jurisdictions or 90% of the jurisdictions assessed was identified fraud as a major money laundering risk. The rate of fraud is increasing all over the world – for example in Singapore, the number of cyber fraud cases has increased by 61% in two years.

In the United Kingdom, fraud now accounts for over 40% of all crime. Several countries estimate that up to 15% of their adult population has fallen victim to a successful cyber fraud attempt, underscoring the widespread and growing nature of this threat.

At the global level is calculated the Global Fraud Index (GFI), which evaluated 112 countries based on four weighted pillars to provide a comprehensive overview of fraud risk and how prepared each country is to access the necessary KYC/AML services (The Sumsuber, 2025):

1. **Fraud Activity (50%)** measures the severity of fraudulent activity, factoring in fraud networks, and AML rates.
2. **Resource Accessibility (20%)** reflects access to digital services and financial power, using indicators like GDP per capita, internet speed, and purchasing power.
3. **Government Intervention (20%)** evaluates regulatory anti-fraud commitment, infrastructure, and resilience through seven governance and policy metrics.
4. **Economic Health (10%)** tracks factors in instability such as corruption, cost of living, unemployment, and economic decline, which may rationalize fraudulent behavior.

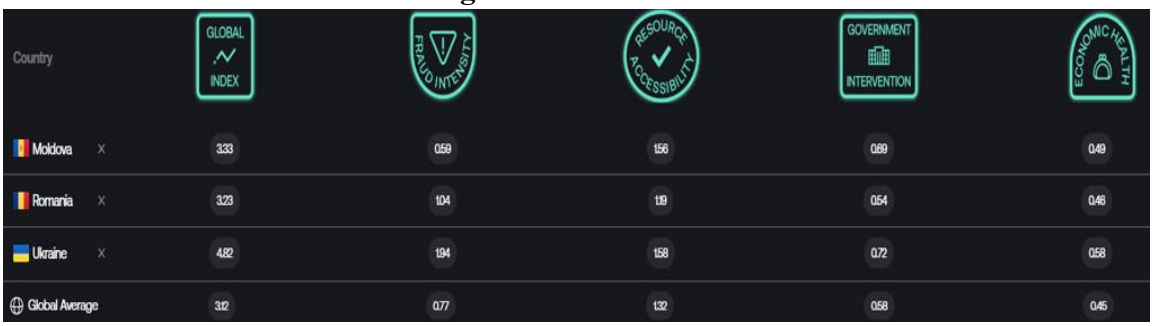
Table 1. Global Fraud Index in regional context for 2025

Country	Global Fraud Index	Fraud Activity	Resource Accessibility	Government Intervention	Economic Health	Rank
Moldova	2.53 ↓	0.57 ↓	1.58 ↑	0.74 ↑	0.49	59
Romania	2.69 ↓	1.08 ↑	1.21 ↑	0.57 ↑	0.46	65
Ukraine	3.71 ↓	1.62 ↓	1.63 ↑	0.78 ↑	0.53 ↓	89
Global Average	2.79	2.07	1.38	0.65	0.46	

***Source**: The Sumsuber (2025)*

In regional context, Global Fraud Index for Moldova in 2025 was equal to 2.53, which compared to the neighbors - Romania and Ukraine is lower, where this indicator constituted: for Romania – 2.69 and for Ukraine – 3.71. In 2025, in Moldova was registered an increase by 0.05 compared to 2024 of government intervention, being equal to 0.74 (see table 1).

Table. 2. Global Fraud Index in regional context for 2024



***Source**: The Sumsuber (2025)*

In the Report on police activity for 2025 (General Police Inspectorate, 2026) the total number of fraud cases increased by 16.62% in 2025 compared to 2024, being registered 3345 cases. The National Bank of Moldova (2026) published on the official website that cyber- enabled fraud have an increasing trend and recommended practical actions how to prevent and protect against fraud.

According to figure 7, there is an increasing trend of cyber-enabled fraud in 2025 compared to 2024, being registered 1225 cases (+47% compared to 2024).

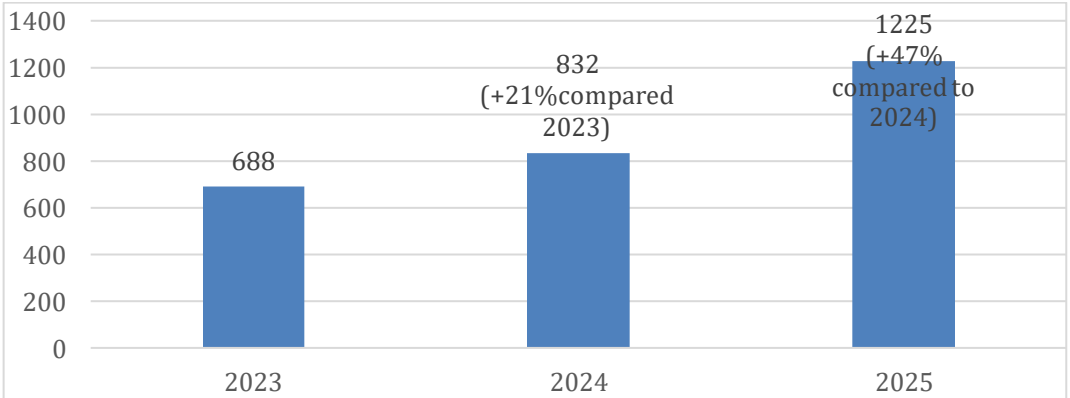


Figure 7. Dynamics of cyber-enabled fraud cases registered in Moldova 2023 -2025

***Source**: elaborated by the author*

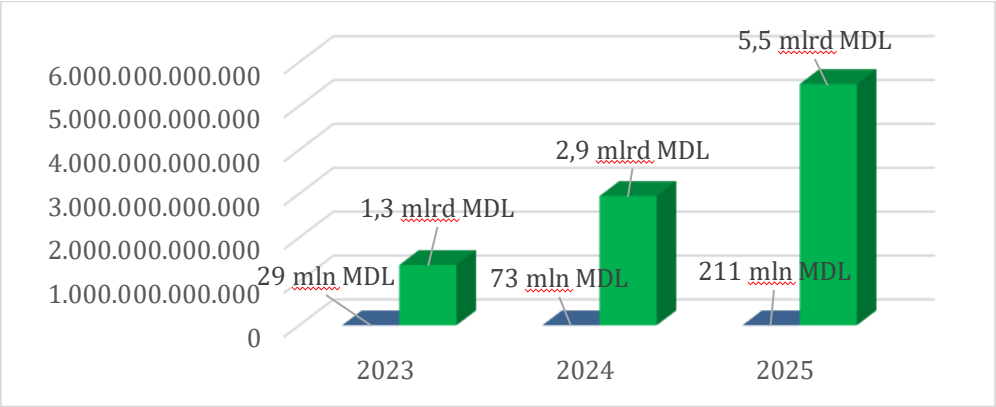


Figure 8. Value dynamics of cyber-enabled fraud in Moldova vs Europe 2023 -2025

***Source**: elaborated by the author*

Analyzing the value dynamics of cyber-enabled fraud in Moldova vs Europe presented in fig.8 we can reveal that in 2025 the value of frauds constituted 211 mln MDL, which is more than in 2024 by 138 mln MDL, and by 182 mln MDL compared to 2023. The cyber-enabled fraud is evolving rapidly being necessary urgent measures from the state authorities, reporting entities (banks, microfinance organizations, etc.) in order to prevent and combat fraud.

How to protect yourself from electronic fraud?

1. Never transmit personal account information: password, CVV code, card expiration date or other sensitive information;
2. Read your monthly statements promptly and carefully. Contact your bank or other financial institution immediately if you identify unauthorized transactions or errors;
3. Never tell anyone your Online Banking password, not even to bank representatives. When you have completed your online banking session, log out and close the browser window. If you suspect fraud or suspicious activity, notify your bank immediately.
4. Choose a "strong" password that is not easily guessed. Try to have at least eight characters in your password, including letters, numbers, and symbols, such as the exclamation mark or pound sign. Change your password regularly.
5. Make sure you know and trust the merchant/vendor before disclosing any information regarding your payment account or pre-authorization of your account, etc.

5. Conclusions

1. In Moldova, cyber-enabled frauds recorded an increasing trend in 2025 compared to 2024 by 47%, with 1225 cases recorded;
2. The Global Fraud Index for Moldova registered a decreasing trend in 2025 compared to 2024 from 3.33 to 2.53 due to government intervention which increased in 2025 compared to 2024 from 0.69 to 0.74.
3. The most common cyber-enabled frauds are related to: fake investment platforms, the use of money mules/droppers; shopping fraud.

4. To protect ourselves from cyber-enabled frauds, it is necessary not to transmit personal account data or other sensitive banking information to unknown persons and not to access unknown links.
5. For financial institutions it is very important in preventing and combatting cyber-enalbed fraud to:
   - to digitize control processes
   - to organize continuous Anti-Fraud &AML training with the employees
   - to organize customer information campaigns

6. References

Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2018). *Fraud examination* (6th ed.). Cengage Learning.

Casey, E. (2019). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (4th ed.). Academic Press.

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Financial Action Task Force. (2025). *Cyber-enabled fraud: Digitalisation and money laundering, terrorist financing and proliferation financing risks*. FATF.

General Police Inspectorate. (2026). *Report on police activity for the year 2025*.

https://politia.md/sites/default/files/media/documents/2026-03/34-1-346%20int.%2016.01.2026.pdf

Glenny, M. (2011). *DarkMarket: Cyberthieves, cybercops and you*. Vintage Books.

Goodman, M. (2015). *Future crimes: Inside the digital underground and the battle for our connected world*. Doubleday.

Holt, T. J., & Bossler, A. M. (2020). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.

INTERPOL. (2026). *Global financial fraud threat assessment* (2nd ed.). https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

National Bank of Moldova. (2026). *NBM recommendation: information from official sources - protection against financial fraud schemes.*

https://www.bnm.md/en/content/nbm-recommendation-information-official-sources-protection-against-financial-fraud-schemes

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

Schneier, B. (2012). *Liars and outliers: Enabling the trust that society needs to thrive*. Wiley.

The Sumsuber. (2025). The Sumsuber - The first expert led media on compliance & anti-fraud. Global Fraud Index: Initial Insights and What You Need to Know in 2025. https://sumsub.com/blog/global-fraud-index-initial-insights/

Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection* (5th ed.). Wiley.

Yar, M. (2018). *Cybercrime and society* (3rd ed.). SAGE Publications