

## Beyond Compliance: Building Financial and Anti-Fraud Resilience in the Digital Economy

Igor Korzhevskiy<sup>1</sup>

<sup>1</sup>Ph.D. (Management), Director, NGO "Global Security", LTD «Risk-Control», Boryspil, Ukraine, ORCID: <https://orcid.org/0000-0003-3012-0735>

### Citation:

Korzhevskiy, I. (2026). Beyond Compliance: Building Financial and Anti-Fraud Resilience in the Digital Economy. *Public Administration and Law Review*, (2(26), 30–41. <https://doi.org/10.36690/2674-5216-2026-2-30-41>

Received: June 01, 2026

Approved: June 29, 2026

Published: June 30, 2026



This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY-NC 4.0\) license](#)



**Abstract.** Financial and anti-fraud resilience has become a critical condition for organisational sustainability, financial stability and public trust in the digital economy. Fraud is increasingly adaptive, technologically enabled and socially manipulative, involving cyber-enabled fraud, payment scams, identity theft, business email compromise, insider misconduct, corruption, cryptocurrency fraud and social engineering. Therefore, fraud should be analysed not only as a compliance violation or criminal act, but also as a systemic resilience challenge that affects organisations, consumers and financial institutions. The objective of this article is to develop an integrated analytical framework for financial and anti-fraud resilience and to identify the governance, regulatory, technological and organisational mechanisms that enable institutions to prevent, detect, respond to and recover from fraud-related financial shocks. The study applies qualitative conceptual analysis, regulatory document analysis and secondary statistical analysis. The research is based on verified reports, standards and regulatory materials produced by ACFE, COSO, the Basel Committee on Banking Supervision, FATF, EBA, ECB, ENISA, FTC, FBI IC3 and UK Finance. The article proposes the Financial and Anti-Fraud Resilience Chain, which includes preparedness, prevention, detection, response, recovery, and learning. It also develops the Financial and Anti-Fraud Resilience Architecture, consisting of governance, control, intelligence, response and learning layers. The results show that effective resilience requires board oversight, ethical culture, fraud risk assessment, internal controls, strong authentication, transaction monitoring, whistleblowing channels, AML integration, incident response, customer protection and post-incident learning. Financial resilience and anti-fraud resilience are mutually dependent. Fraud weakens financial stability, while weak financial resilience reduces the capacity to invest in fraud prevention, detection and recovery systems. Further research should focus on AI-based fraud detection, behavioural vulnerabilities in authorised scams, reimbursement models, fraud risks in instant payments and cryptocurrencies, and the impact of deepfakes and synthetic identities on financial security.

**Keywords:** financial resilience; anti-fraud resilience; fraud risk management; financial crime; cyber-enabled fraud; internal controls; operational resilience; payment fraud; digital financial security; money laundering; fraud detection; institutional trust.

**JEL Classification:** G21; G28; G32; G38; K42; M42; O33.

**Formulas:** 0; **fig.:** 1; **tabl.:** 3; **bibl.:** 17

**Introduction.** Financial and anti-fraud resilience has become a strategic priority for organisations, financial institutions, regulators and societies. In the digital economy, fraud is no longer limited to isolated acts of deception, internal theft or falsified documents. It has evolved into a complex and adaptive system of risks involving cyber-enabled fraud, authorised push payment scams, identity theft, social engineering, insider misconduct, corruption, payment manipulation, synthetic identities, business email compromise, cryptocurrency fraud and platform-enabled deception. As a result, financial resilience and anti-fraud resilience must be understood together.

Financial resilience refers to the ability of an organisation, financial system or household to withstand financial shocks, preserve liquidity, maintain critical operations and recover after disruption. Anti-fraud resilience refers to the ability to prevent, detect, respond to and learn from fraudulent activity. These two forms of resilience are interconnected. Fraud weakens financial stability, destroys trust, increases operational costs, reduces consumer confidence and may trigger legal, reputational and regulatory consequences. At the same time, financially weak organisations are more vulnerable to fraud because they may underinvest in internal controls, cybersecurity, staff training, monitoring and investigation capacity.

The scale of the problem is significant. The Federal Trade Commission reported that U.S. consumers lost more than \$12.5 billion to fraud in 2024, a 25% increase compared with the previous year (Federal Trade Commission, 2025). The FBI Internet Crime Complaint Center reported \$16.6 billion in losses from internet crime in 2024, with investment fraud involving cryptocurrency producing the largest losses, more than \$6.5 billion (Federal Bureau of Investigation, 2025). In Europe, the European Banking Authority and the European Central Bank reported that payment fraud across the European Economic Area amounted to €4.3 billion in 2022 and €2.0 billion in the first half of 2023 (European Banking Authority & European Central Bank, 2024). In the United Kingdom, UK Finance reported that £1.17 billion was lost to fraud in 2023 (UK Finance, 2024).

These figures show that fraud is not only a criminal or compliance issue. It is a resilience issue. Organisations and financial systems must be able not only to comply with rules, but also to anticipate evolving schemes, detect weak signals, protect customers, maintain operations, cooperate with regulators and recover trust after incidents. Therefore, the central argument of this article is that financial and anti-fraud resilience should be built as an integrated governance system, combining financial controls, operational resilience, cybersecurity, behavioural awareness, data analytics, regulatory compliance and institutional learning.

**Literature review.** The academic and professional literature on fraud has traditionally focused on motivation, opportunity and rationalisation. The fraud triangle, developed from the work of Cressey, explains fraudulent

behaviour through pressure, opportunity and rationalisation (Cressey, 1953). Later models, including the fraud diamond, added capability as an important factor because not every person with pressure, opportunity and rationalisation can successfully commit fraud (Wolfe & Hermanson, 2004). These models remain relevant because they show that fraud prevention must reduce opportunities, change incentives, strengthen ethical culture and limit the capacity to exploit weaknesses.

However, the digital transformation of finance requires a broader approach. Fraud is increasingly organised, data-driven, technologically enabled and cross-border. Social engineering allows criminals to manipulate victims into authorising transactions themselves. Business email compromise exploits trust relationships within organisations. Phishing, smishing and deepfake techniques reduce the effectiveness of traditional authentication. Cryptocurrency and virtual assets create new channels for laundering proceeds and moving funds quickly. Therefore, anti-fraud systems must combine internal control, cyber resilience, behavioural risk management and intelligence-led monitoring.

The Association of Certified Fraud Examiners defines occupational fraud as fraud committed by individuals against their employing organisations. Its 2024 Report to the Nations is based on 1,921 real cases from 138 countries and territories and estimates that organisations lose approximately 5% of revenue to fraud each year (Association of Certified Fraud Examiners, 2024). The report also shows that asset misappropriation is the most common occupational fraud category, while financial statement fraud is less frequent but more costly. This confirms that organisations need differentiated controls for different fraud types.

The COSO and ACFE Fraud Risk Management Guide provides a structured approach to fraud risk governance. It emphasises governance, fraud risk assessment, prevention, detection, investigation and corrective action (COSO & Association of Certified Fraud Examiners, 2023). This approach is important because it moves fraud management from reactive investigation to enterprise-wide risk management. Fraud resilience is not achieved only by detecting fraud after losses occur. It requires a permanent system of controls, accountability and learning.

Operational resilience literature also contributes to the topic. The Basel Committee on Banking Supervision defines operational resilience as the ability of a bank to deliver critical operations through disruption (Basel Committee on Banking Supervision, 2021). Although Basel's principles focus on banking and operational disruptions, they are directly relevant to financial and anti-fraud resilience because fraud incidents can disrupt payment systems, customer access, internal operations, liquidity management and public confidence. The Basel approach emphasises governance, operational risk management, business continuity, third-party dependency management, incident management and testing.

Regulatory literature increasingly connects fraud, cybersecurity and digital operational resilience. In the European Union, the Digital Operational Resilience Act requires financial entities to manage information and communication technology risks, report major incidents, test digital resilience and manage third-party ICT risks (European Parliament & Council of the European Union, 2022). DORA became applicable in January 2025 and reflects a shift from narrow IT compliance to systemic digital resilience. This is particularly relevant because fraud often exploits digital channels, third-party dependencies and weak authentication processes.

The FATF perspective adds another dimension: fraud proceeds often become money laundering risks. FATF research on methods and trends shows that criminals exploit digitalisation, cyber-enabled crime, virtual assets and cross-border structures to move and conceal illicit funds (Financial Action Task Force, 2024). Thus, anti-fraud resilience must be integrated with anti-money laundering and counter-terrorist financing controls. Fraud detection cannot end at the point of loss recognition. It must include tracing funds, suspicious activity reporting, customer due diligence and cooperation with law enforcement.

Finally, consumer protection literature shows that fraud resilience is not limited to organisations. Individuals and households are also affected. Fraud may cause not only direct financial loss, but also psychological harm, shame, distrust and reduced willingness to use digital services. Therefore, financial and anti-fraud resilience must include consumer education, safe digital design, reimbursement rules, rapid reporting channels and victim support.

**Aims.** The aim of this article is to develop an integrated analytical framework for financial and anti-fraud resilience and to identify the governance, regulatory, technological and organisational mechanisms that enable institutions to prevent, detect, respond to and recover from fraud-related financial shocks.

**Methodology.** The article uses qualitative conceptual analysis, regulatory document analysis and secondary statistical analysis. The research is based on verified reports, standards and regulatory materials produced by international organisations, financial regulators, professional anti-fraud associations and public enforcement agencies.

The sources include the ACFE Report to the Nations, COSO and ACFE Fraud Risk Management Guide, Basel Committee principles for operational resilience, FATF materials on financial crime risks, EBA and ECB payment fraud reports, ENISA cybersecurity threat landscape reports, FTC Consumer Sentinel Network data, FBI IC3 Internet Crime Report, UK Finance Annual Fraud Report and EU DORA regulatory materials.

The methodology is based on functional analysis rather than simple comparison by country. The article identifies the institutional functions required for resilience and organises them into a resilience chain. This approach is used because fraud evolves dynamically and crosses

organisational, technological and jurisdictional boundaries. Therefore, the central question is not only where fraud happens, but how institutions can build capabilities to withstand and adapt to it.

The chain shows that resilience is not a single control or one-time compliance exercise. It is a continuous cycle in which organisations prepare for fraud risks, prevent avoidable losses, detect suspicious activity, respond quickly, recover financial and operational stability, and transform experience into improved controls.

**Results.** Financial resilience and anti-fraud resilience overlap, but they are not identical. Financial resilience concerns the ability to maintain financial viability under pressure. It includes liquidity, capital adequacy, revenue stability, cost control, insurance, contingency planning and continuity of critical operations. Anti-fraud resilience concerns the ability to resist fraud attempts, reduce exposure, detect anomalies, protect victims, investigate incidents and learn from failures.

The relationship between these concepts is reciprocal. Fraud can weaken financial resilience by creating direct losses, legal costs, regulatory fines, compensation obligations and reputational damage. Weak financial resilience can weaken anti-fraud controls because organisations under financial pressure may reduce spending on compliance, audit, security and training. Therefore, resilience must be designed as an integrated system.

**Table 1. Relationship between financial resilience and anti-fraud resilience**

| Dimension        | Financial resilience                                             | Anti-fraud resilience                                                     | Integrated effect                                          |
|------------------|------------------------------------------------------------------|---------------------------------------------------------------------------|------------------------------------------------------------|
| Core purpose     | Preserve financial stability                                     | Prevent and reduce fraud losses                                           | Protection of financial continuity and trust               |
| Main risks       | Liquidity shocks, revenue decline, operational disruption        | Internal fraud, external scams, cyber-enabled fraud, payment manipulation | Reduced vulnerability to financial crime shocks            |
| Main instruments | Capital buffers, liquidity planning, insurance, continuity plans | Internal controls, monitoring, investigation, reporting, staff awareness  | Stronger capacity to absorb and respond to fraud incidents |
| Governance focus | Board oversight of financial risk                                | Board oversight of fraud risk and ethical culture                         | Enterprise-wide resilience governance                      |
| Main outcome     | Ability to withstand financial pressure                          | Ability to resist and recover from fraud                                  | Sustainable institutional trust                            |

*Source: developed by the author based on Basel Committee on Banking Supervision (2021), COSO and Association of Certified Fraud Examiners (2023), and Association of Certified Fraud Examiners (2024).*

**Fraud as an adaptive risk.** Fraud is adaptive because fraudsters respond to controls. When authentication improves, criminals may move from unauthorised access to authorised payment manipulation. When organisations strengthen technical controls, criminals may use social engineering. When card fraud becomes harder, fraudsters may target instant payments, investment platforms or cryptocurrency channels. This adaptive nature makes fraud resilience different from static compliance.

The EBA and ECB report confirms that strong customer authentication has had a beneficial effect on fraud levels, especially in card fraud, but payment fraud remains significant across the European Economic Area (European Banking Authority & European Central Bank, 2024). This suggests that technical safeguards are necessary, but fraudsters continuously shift tactics toward areas where human behaviour, urgency, trust and digital complexity can be exploited.

ENISA also identifies the financial sector as a major target for cyber threats. Its financial sector threat landscape highlights mobile malware fraud, smishing, malicious applications and attacks against digital banking users (ENISA, 2025). This confirms that anti-fraud resilience must include cyber threat intelligence, customer behaviour monitoring and digital literacy.

**Statistical evidence on fraud losses.** Verified international data show the scale and diversity of fraud-related losses.

**Table 2. Selected verified statistical evidence on fraud and financial crime**

| Indicator                                                   | Value                                                       | Source                          |
|-------------------------------------------------------------|-------------------------------------------------------------|---------------------------------|
| Reported U.S. consumer fraud losses in 2024                 | More than \$12.5 billion                                    | Federal Trade Commission        |
| Increase in reported U.S. fraud losses compared with 2023   | 25%                                                         | Federal Trade Commission        |
| FBI IC3 reported internet crime losses in 2024              | \$16.6 billion                                              | Federal Bureau of Investigation |
| Largest FBI IC3 loss category in 2024                       | Cryptocurrency-related investment fraud, over \$6.5 billion | Federal Bureau of Investigation |
| EEA payment fraud in 2022                                   | €4.3 billion                                                | EBA and ECB                     |
| EEA payment fraud in the first half of 2023                 | €2.0 billion                                                | EBA and ECB                     |
| UK fraud losses in 2023                                     | £1.17 billion                                               | UK Finance                      |
| ACFE 2024 occupational fraud study                          | 1,921 cases from 138 countries and territories              | ACFE                            |
| Estimated annual organisational revenue lost to fraud       | 5%                                                          | ACFE                            |
| Asset misappropriation share of occupational fraud cases    | 89%                                                         | ACFE                            |
| Corruption share of occupational fraud cases                | 48%                                                         | ACFE                            |
| Financial statement fraud share of occupational fraud cases | 5%                                                          | ACFE                            |

*Source: compiled by the author based on Federal Trade Commission (2025), Federal Bureau of Investigation (2025), European Banking Authority and European Central Bank (2024), UK Finance (2024), and Association of Certified Fraud Examiners (2024).*

The data show three important patterns. First, consumer and cyber-enabled fraud losses are rising rapidly. Second, payment fraud remains a material risk even in highly regulated markets. Third, occupational fraud remains a persistent organisational risk, with internal controls and ethical culture playing decisive roles.

**The Financial and Anti-Fraud Resilience Architecture.** Based on the analysis, financial and anti-fraud resilience can be systematised into five institutional layers.

**Table 3. Financial and Anti-Fraud Resilience Architecture**

| Layer              | Purpose                                     | Key instruments                                                                                           | Resilience contribution                      |
|--------------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Governance layer   | Establish accountability and risk ownership | Board oversight, fraud risk appetite, ethics policies, three lines model                                  | Defines responsibility and strategic control |
| Control layer      | Reduce opportunities for fraud              | Segregation of duties, approvals, reconciliations, access controls, strong authentication                 | Prevents avoidable losses                    |
| Intelligence layer | Detect anomalies and emerging threats       | Data analytics, transaction monitoring, whistleblowing, threat intelligence, customer behaviour analytics | Improves early detection                     |
| Response layer     | Limit harm after fraud occurs               | Incident response, investigations, reporting, freezing funds, law enforcement cooperation                 | Reduces financial and reputational damage    |
| Learning layer     | Improve the system after incidents          | Root cause analysis, control redesign, staff training, scenario testing, lessons learned                  | Builds adaptive resilience                   |

*Source: developed by the author based on COSO and Association of Certified Fraud Examiners (2023), Basel Committee on Banking Supervision (2021), European Parliament and Council of the European Union (2022), and ENISA (2025).*

This architecture differs from traditional compliance models because it treats fraud as a dynamic system risk. The governance layer ensures responsibility. The control layer reduces exposure. The intelligence layer identifies weak signals. The response layer limits harm. The learning layer creates adaptation.

**Prevention mechanisms.** Fraud prevention begins with governance. The board and senior management must define fraud risk appetite, establish ethical expectations and ensure that fraud risk is included in enterprise risk management. COSO and ACFE emphasise that fraud risk management requires governance, fraud risk assessment, prevention, detection, investigation and corrective action (COSO & Association of Certified Fraud Examiners, 2023).

Prevention also requires internal controls. Segregation of duties, dual authorisation, vendor verification, employee screening, access management, transaction limits and reconciliation processes reduce fraud opportunities. However, controls must be risk-based. Excessive control may reduce operational efficiency, while weak control increases fraud exposure.

Digital fraud prevention requires strong customer authentication, secure onboarding, device intelligence, transaction risk analysis, confirmation of payee, customer warnings and behavioural analytics. The EBA and ECB report confirms the beneficial impact of strong customer authentication on

fraud levels (European Banking Authority & European Central Bank, 2024). However, authentication alone cannot prevent authorised scams because victims may be manipulated into approving transactions.

Human-centred prevention is equally important. Fraudsters exploit emotions such as fear, urgency, greed, trust, shame and hope. Therefore, staff and customer education should focus not only on technical rules, but also on behavioural red flags: pressure to act quickly, requests for secrecy, unusual payment instructions, unexpected changes in bank details, emotional manipulation and promises of unrealistic returns.

**Detection mechanisms.** Fraud detection depends on the ability to identify abnormal patterns. Traditional detection relies on internal audit, management review, reconciliations and whistleblowing. Digital detection uses data analytics, machine learning, network analysis, device fingerprinting, geolocation anomalies, behavioural biometrics and transaction monitoring.

The ACFE has consistently found that tips are among the most common detection methods in occupational fraud cases, which confirms the importance of whistleblowing channels and speak-up culture (Association of Certified Fraud Examiners, 2024). A hotline is not merely a reporting tool. It is a signal that the organisation expects transparency and protects those who report concerns.

Detection must also be linked to anti-money laundering monitoring. Fraud proceeds often move quickly through mule accounts, cryptocurrency wallets, shell companies or cross-border transfers. FATF emphasises the importance of understanding evolving criminal methods and applying risk-based mitigation measures (Financial Action Task Force, 2024). Therefore, fraud teams and AML teams should not work in isolation.

**Response and recovery mechanisms.** Fraud response must be fast, coordinated and evidence-based. The first priority is containment: stopping transactions, freezing accounts, preserving evidence and preventing further loss. The second priority is investigation: identifying the fraud mechanism, responsible actors, control failures and affected parties. The third priority is reporting: notifying regulators, law enforcement, insurers, customers and internal governance bodies when required. The fourth priority is recovery: recovering funds, compensating victims where appropriate, restoring operations and rebuilding trust.

Operational resilience principles are especially relevant in this stage. Basel's principles focus on the ability to deliver critical operations through disruption (Basel Committee on Banking Supervision, 2021). Fraud incidents may not always stop operations, but severe incidents can affect customer access, liquidity, payment processing and public confidence. Therefore, fraud response should be connected with business continuity planning and crisis communication.

In the EU financial sector, DORA strengthens this connection by requiring financial entities to manage ICT risks, classify and report incidents, test resilience and manage third-party providers (European Parliament & Council of the European Union, 2022). This is important because many fraud incidents involve technological systems, outsourced platforms or digital service providers.

**Learning and adaptation.** The final stage of resilience is learning. Organisations often focus on closing an individual case, but resilience requires deeper analysis. After a fraud incident, the organisation should ask several questions: What vulnerability was exploited? Was it a control failure, governance failure, human factor, technological weakness or external dependency? Were warning signs ignored? Was the response timely? Did staff understand reporting procedures? Did customers receive effective warnings? Did third parties contribute to the risk?

Learning requires root cause analysis, control redesign, staff retraining, updated risk scenarios, board reporting and testing. Fraud scenarios should be included in stress testing and crisis simulations. This is particularly important because fraud schemes evolve quickly and may combine cyber intrusion, social engineering, insider assistance and money laundering.

**Discussion.** The results demonstrate that financial and anti-fraud resilience should be understood as an integrated governance capability rather than a set of isolated controls. The main challenge is that fraud is adaptive, cross-functional and increasingly digital. It does not respect organisational boundaries between finance, compliance, cybersecurity, operations, customer service and legal departments. Therefore, resilience requires coordination across all these areas.

The first major implication is that compliance is necessary but insufficient. Organisations may formally comply with regulations and still remain vulnerable if controls are poorly designed, staff are not trained, data are fragmented, whistleblowers are not protected or customer warnings are ineffective. Fraud resilience requires an operational culture in which prevention and detection are embedded in daily processes.

The second implication is that fraud risk must be treated as a board-level risk. Fraud can create direct financial losses, regulatory sanctions, litigation, reputational harm and loss of trust. Boards should therefore receive regular information on fraud typologies, loss trends, control weaknesses, investigation outcomes and emerging threats. Fraud risk appetite should be explicit and linked with internal controls, digital strategy and customer protection.

The third implication concerns data. Fraud detection increasingly depends on high-quality, timely and interoperable data. However, data analytics alone cannot solve fraud. Algorithms may identify suspicious patterns, but human expertise is needed to interpret context, understand deception, investigate intent and avoid unfair treatment of customers.

Therefore, the future of fraud resilience lies in combining technology with professional judgement.

The fourth implication concerns customers and citizens. Fraud prevention cannot be shifted entirely onto victims. Many scams are designed by professional criminals who exploit psychological pressure, trusted brands and digital complexity. Financial institutions, platforms, telecom providers and regulators should share responsibility for prevention. This includes safer system design, confirmation tools, transaction warnings, rapid reporting, reimbursement frameworks and public education.

The fifth implication concerns the relationship between fraud and cyber risk. Phishing, ransomware, malware, account takeover and business email compromise demonstrate that cyber incidents and fraud losses are increasingly connected. ENISA's threat landscape identifies phishing, malware, ransomware and social engineering as persistent threats (ENISA, 2024, 2025). Therefore, anti-fraud resilience should be integrated with cybersecurity and digital operational resilience.

The sixth implication concerns third-party risk. Financial institutions increasingly rely on cloud providers, payment processors, fintech partners, data vendors and outsourced service providers. DORA addresses this issue by strengthening ICT third-party risk management in the EU financial sector (European Parliament & Council of the European Union, 2022). Fraud resilience requires visibility over third-party controls, incident response procedures, contractual obligations and concentration risks.

The seventh implication concerns social trust. Fraud weakens trust not only in individual organisations, but also in financial systems and digital transformation. If consumers believe that online banking, digital payments or investment platforms are unsafe, they may reduce participation in the digital economy. Thus, anti-fraud resilience supports financial inclusion and digital confidence.

The article's analytical contribution is the Financial and Anti-Fraud Resilience Chain. It shows that resilience is built through six connected stages: preparedness, prevention, detection, response, recovery, and learning. If any stage is weak, the whole system becomes vulnerable. For example, strong detection without recovery may leave victims unsupported. Strong prevention without learning may become obsolete. Strong response without preparedness may be slow and fragmented.

**Conclusions.** Financial and anti-fraud resilience is a critical condition for organisational sustainability, financial stability and public trust in the digital economy. Fraud has become more adaptive, technologically enabled and socially manipulative. It affects organisations, consumers, financial institutions and public systems. Therefore, fraud should be treated not only as a compliance violation or criminal act, but also as a resilience challenge.

The article shows that financial resilience and anti-fraud resilience are mutually dependent. Fraud undermines financial resilience through losses,

finances, compensation costs and reputational damage. Weak financial resilience undermines anti-fraud capacity by reducing investment in controls, monitoring and training. Effective resilience requires their integration into one governance system.

The proposed Financial and Anti-Fraud Resilience Chain includes preparedness, prevention, detection, response, recovery, and learning. This chain allows organisations to move from reactive fraud management to adaptive resilience. The Financial and Anti-Fraud Resilience Architecture further identifies five layers: governance, control, intelligence, response and learning. Together, these models provide a practical framework for organisations and regulators.

The analysis confirms that effective anti-fraud resilience requires board oversight, ethical culture, fraud risk assessment, internal controls, strong authentication, data analytics, whistleblowing channels, AML integration, incident response, customer protection and post-incident learning. It also requires cooperation between financial institutions, regulators, law enforcement, technology providers, platforms and consumers.

Further research should focus on measuring the effectiveness of anti-fraud resilience frameworks, evaluating AI-based fraud detection, assessing behavioural vulnerabilities in authorised scams, comparing reimbursement models, analysing fraud risks in instant payments and cryptocurrencies, and studying the psychological and social consequences of fraud victimisation. Special attention should also be given to the role of artificial intelligence, deepfakes and synthetic identities in future fraud ecosystems.

**Conflict of interest.** The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

**Funding.** The author declares that no financial support was received for the research, authorship, and/or publication of this article.

**Ethics statement.** All procedures performed in this study complied with institutional and international ethical standards.

**Generative AI statement.** The author declares that no Generative AI was used in the creation of this manuscript.

**Publisher's note.** All claims expressed in this article are solely those of the author's and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

## References:

1. Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations. <https://legacy.acfe.com/report-to-the-nations/2024/>
2. Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d516.htm>
3. Basel Committee on Banking Supervision. (2022). Principles for operational resilience: Executive summary. Bank for International Settlements. [https://www.bis.org/fsi/fsisummaries/op\\_resilience.htm](https://www.bis.org/fsi/fsisummaries/op_resilience.htm)

4. COSO, & Association of Certified Fraud Examiners. (2023). Fraud risk management guide (2nd ed.). <https://downloads.ctfassets.net/rb9cdnjh59cm/38niR1KQg3knFZBp7rMmwb/1458f67994b694bccca63d1e5bbbf9f1/COSO-Fraud-Risk-Management-Guide-2023.pdf>
5. Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.
6. ENISA. (2024). ENISA threat landscape 2024. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
7. ENISA. (2025). ENISA threat landscape: Finance sector. European Union Agency for Cybersecurity. [https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024\\_Final.pdf](https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf)
8. European Banking Authority, & European Central Bank. (2024). 2024 report on payment fraud. <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf>
9. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
10. Federal Bureau of Investigation. (2025). FBI releases annual Internet Crime Report. <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>
11. Federal Trade Commission. (2025). New FTC data show a big jump in reported losses to fraud to \$12.5 billion in 2024. <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
12. Financial Action Task Force. (2024). Methods and trends. <https://www.fatf-gafi.org/en/topics/methods-and-trends.html>
13. Financial Action Task Force. (2026). Fraud warning. <https://www.fatf-gafi.org/en/pages/fraud-warning.html>
14. Mihus, I. (2026). Information and analytical support for partner verification in the enterprise economic security system based on international standards. *Economics and Management*, 1, 35-41. <https://doi.org/10.32782/2312-7872.1.2026.5>
15. UK Finance. (2024). Annual fraud report 2024. <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024>
16. U.S. Federal Trade Commission. (2024). Consumer Sentinel Network Data Book 2024. <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>
17. Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38-42.