

FRAUD IN ELECTRONIC COMMERCE UNDER THE DIGITALISATION OF ECONOMIC RELATIONS: CRIMINAL LAW CHALLENGES AND ECONOMIC IMPLICATIONS FOR DIGITAL MARKETS

Andrii Babenko¹, Andriy Dzyurbel², Denys Illiashchuk³

Abstract. The rapid digitalisation of economic relations and the growth of e-commerce have fundamentally changed business models, financial transactions and consumer behaviour. However, alongside these positive developments, digital markets have also become increasingly vulnerable to sophisticated fraud exploiting information technologies, online payment systems, virtual assets and cross-border electronic communications. Consequently, fraud in electronic commerce has evolved from being merely a criminal law issue to becoming a significant factor affecting the economic security, investment attractiveness and sustainable development of digital markets.

The purpose of this study is twofold: first, to identify the main issues surrounding the criminal law qualification of fraud in electronic commerce in the context of digital transformation; and second, to evaluate the economic implications of these issues for the development of the digital market. The study takes a multidisciplinary approach, combining doctrinal legal analysis with the principles of law and economics. A comparative analysis of legal, formal-legal, institutional and case law is employed to examine Ukrainian criminal legislation, judicial practice and contemporary scientific approaches to cyber fraud. The research also considers the economic consequences of legal uncertainty for electronic commerce, such as increased transaction costs, reduced consumer confidence, higher compliance expenditure and obstacles to the development of the digital market.

The findings show that the lack of a comprehensive legal definition of cyber fraud, inconsistent judicial interpretations and outdated legislative terminology make it much more difficult to qualify fraudulent conduct in electronic commerce as a criminal offence. Particular difficulties arise in distinguishing between fraud and civil law disputes, unauthorised electronic transactions, theft involving payment instruments and offences relating to virtual assets. The research also shows that legal uncertainty has a negative impact on the functioning of digital markets, increasing business risks, discouraging investment and undermining public trust in online commercial transactions. The study concludes that improving criminal legislation should be regarded not only as a means of strengthening the criminal justice system, but also as an important tool for promoting economic security and fostering the growth of a sustainable digital market. Legislative modernisation, harmonisation of judicial practice, clearer qualification criteria, and improved international co-operation in digital evidence collection would contribute to reducing transaction costs, strengthening legal certainty, and increasing the competitiveness of the digital economy.

Keywords: electronic commerce, fraud, cyber fraud, criminal law qualification, digital economy, economic security, digital markets, transaction costs, virtual assets, cybercrime, pre-trial investigation, evidence, proving, crimes, unsolved crimes.

JEL Classification: K14, K24, K42, O33

Received on: June 17, 2026 **Accepted on:** August 19, 2026 **Published on:** September 28, 2026

¹ Odesa State University of Internal Affairs, Ukraine (*corresponding author*)

E-mail: an.babenko@ukr.net

ORCID: <https://orcid.org/0000-0002-9498-2484>

² West Ukrainian National University, Ukraine

E-mail: tayfun.77@ukr.net

ORCID: <https://orcid.org/0009-0000-1778-8699>

³ Odesa State University of Internal Affairs, Ukraine

E-mail: illiashchuk.denys@ukr.net

ORCID: <https://orcid.org/0009-0004-2685-9208>



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

1. Introduction

Digital transformation is one of the key factors shaping the development of modern economic systems. The growth of e-commerce, online financial services, digital platforms and automated payment systems has greatly improved the efficiency of economic transactions and broken down traditional barriers between market participants. While digitalisation contributes to productivity growth, innovation development, and the creation of new forms of economic activity, it also generates new risks related to cybersecurity, consumer protection, and trust in digital environments (OECD, 2019).

Electronic commerce relies on economic actors being able to interact remotely via digital platforms, without direct personal contact. While this provides significant economic advantages, it also creates conditions for fraudulent behaviour. The absence of physical interaction, information asymmetry between participants, user anonymity and dependence on technological infrastructure provide offenders with opportunities to manipulate digital transactions and exploit weaknesses in verification systems.

From an economic perspective, fraud in electronic commerce incurs additional costs for businesses, consumers and public institutions. These include investments in cybersecurity technologies, transaction monitoring systems, compliance procedures, insurance mechanisms and legal protection measures. According to institutional economic theory, uncertainty increases transaction costs because market participants must allocate additional resources to mitigate the risks of incomplete information and opportunistic behaviour (Williamson, 1985).

The problem of electronic fraud has become particularly important because traditional criminal law was developed primarily for physical economic relations. The traditional definition of fraud as the act of obtaining property through deception or abuse of trust becomes more complicated when illegal activities involve automated systems, electronic payment platforms, artificial intelligence technologies or blockchain-based assets.

In Ukraine, as in many other jurisdictions, the criminal law surrounding fraud remains based on general legal principles. Article 190 of the Ukrainian Criminal Code defines fraud as the acquisition of another person's property or rights through deception or abuse of trust. However, this provision does not fully reflect the technological characteristics of modern fraudulent schemes, making it difficult to qualify and collect evidence.

A significant challenge lies in distinguishing between criminal fraud and civil law disputes arising from online transactions. In electronic commerce, non-delivery of goods, failure to provide services or refusal to return

payments may constitute either a contractual violation or an intentional fraudulent scheme. The main criterion for criminal prosecution is establishing criminal intent when property is obtained; however, proving such intent in a digital environment is considerably more difficult due to the fragmented and volatile nature of electronic evidence.

Another important issue is fraudulent activity involving electronic payments and virtual assets. While the development of cryptocurrency markets and blockchain technologies has created new forms of economic value, it has also introduced additional risks relating to anonymity, cross-border transactions and the difficulty of recovering illegally obtained assets (Böhme et al., 2015; Foley et al., 2019).

Therefore, electronic fraud should be considered not only as a criminal law issue, but also as a factor that affects the way digital markets function. The level of protection against fraudulent behaviour directly influences consumer trust, business activity and the sustainable development of electronic commerce.

2. Literature Review

The theoretical foundations of digital market development and electronic commerce are closely linked to the concepts of trust and information asymmetry. According to Akerlof's theory of information asymmetry, insufficient information about market participants can result in inefficient economic outcomes and create opportunities for opportunistic behaviour (Akerlof, 1970). This theoretical approach is particularly relevant to electronic commerce, given that consumers often make decisions without having any direct knowledge of the sellers, the quality of the products, or the security of the transactions.

Research on electronic commerce confirms that trust is one of the main factors influencing consumers' willingness to engage in online transactions. Gefen, Karahanna and Straub (2003) demonstrated that trust significantly influences acceptance of online shopping, and Pavlou (2003) emphasised the relationship between perceived risk, trust and adoption of electronic commerce.

Research into cybercrime is increasingly focusing on the economic consequences of digital fraud. Anderson et al. (2019) emphasise that cybercrime results in significant financial losses for individual users and entire economic sectors. Wall (2017) observes that technological advancements have transformed the structure of traditional crime by creating new opportunities for financially motivated offences.

The issue of organised cybercrime has also received considerable attention from academics. Leukfeldt, Lavorgna and Kleemans (2017) contend that contemporary cybercrime frequently entails

a combination of technological expertise and traditional criminal structures, rendering investigation and prevention more challenging.

Cryptocurrency-related fraud is another important area of research. Böhme et al. (2015), for example, analysed Bitcoin as a new financial technology, emphasising both its economic potential and the associated regulatory challenges. Meanwhile, Foley, Karlsen and Putniņš (2019) demonstrated that, due to their pseudonymous nature and global accessibility, cryptocurrencies may also be used for illegal economic activities.

International organisations have increasingly recognised electronic fraud as a threat to the development of the digital economy. Studies by the OECD emphasise that consumer confidence and effective protection mechanisms are essential for the long-term success of electronic commerce (OECD, 2016; OECD, 2022). Reports from the FATF and Europol highlight the growing complexity of cyber-enabled financial crimes and the need for international co-operation in tackling them.

At the national level, Ukrainian researchers have focused mainly on criminal law qualification issues. Recent studies examine problems of applying Article 190 of the Criminal Code of Ukraine to fraud involving electronic technologies, digital evidence, and virtual assets (Reznichenko & Chekmarova, 2024; Usmanov, 2024; Lypkan, 2025). However, the economic dimension of electronic fraud and its influence on digital markets requires further research.

3. Methodology

The study's methodological framework is based on an interdisciplinary approach that combines legal and economic analysis. The research uses institutional economic theory to investigate the impact of legal uncertainty and fraud risks on transaction costs and market efficiency.

A comparative legal analysis was conducted to examine international regulatory approaches to electronic fraud, digital consumer protection, virtual assets and cybersecurity. The formal legal method was then applied to examine the provisions of Ukrainian criminal law governing fraud and related offences.

The study employs a systematic analysis of academic literature, international reports and regulatory documents issued by the OECD, the FATF, Europol and European Union institutions. This approach enables common trends in digital fraud regulation to be identified and directions for improving national legal mechanisms to be determined.

The combination of legal and economic approaches enables the consideration of electronic fraud not only as an individual criminal act, but also as a factor influencing trust, investment activity, transaction

costs, and the sustainable development of digital markets.

4. Results and Discussion

4.1. Criminal Law Qualification of Fraud in Electronic Commerce and Its Impact on Digital Markets

The development of electronic commerce has significantly altered the traditional methods of exchanging property and conducting financial transactions. While digital platforms, online marketplaces and electronic payment systems have created new economic opportunities, they have also given rise to a wider range of fraudulent practices that exploit technological and informational vulnerabilities.

Unlike traditional forms of fraud, electronic commerce fraud is characterised by the absence of direct contact between offender and victim, the use of digital communication channels and the ability to conduct transactions across different jurisdictions. These characteristics make it difficult to establish the elements of a criminal offence, particularly when it comes to identifying the offender, determining how property was obtained, and establishing intent.

From an economic perspective, electronic fraud undermines one of the fundamental building blocks of digital markets: trust. Online commerce depends on consumers having confidence that digital transactions are secure and that market participants are honest. A decrease in trust leads to higher transaction costs, as businesses and consumers need to invest more in verification mechanisms, cybersecurity tools, insurance and dispute resolution procedures (Pavlou, 2003).

The main difficulty in qualifying criminal behaviour lies in distinguishing fraud from ordinary contractual violations. In electronic commerce, situations in which a seller fails to deliver goods or provide services can have different legal ramifications, depending on whether the seller initially intended to steal another person's property.

The decisive criterion is the subjective element of the offence: direct intent to obtain property through deception. If a person receives payment while intending not to fulfil their contractual obligations, this may constitute fraud. However, if the inability to fulfil obligations arises after the agreement is made due to objective circumstances, the dispute generally falls under civil law.

This distinction is particularly important in digital markets, as excessive criminalisation of ordinary commercial disputes could hinder entrepreneurial activity, while inadequate criminal law protection could undermine consumer confidence. Therefore, legal regulation must be balanced and based on clear criteria for distinguishing between criminal and civil liability.

The Supreme Court of Ukraine has repeatedly emphasised that the key factors that distinguish fraud from civil law violations include the intention to obtain property, when the intention was formed, the nature of the actions performed by the individual and whether the dispute can be resolved through civil law mechanisms. This approach aligns with international practices, in which fraudulent intent and dishonest behaviour are central to the qualification of economic crimes.

4.2. Electronic Payment Fraud and the Problem of Distinguishing Fraud from Theft

One of the most controversial issues surrounding digital fraud is the use of electronic payment instruments, such as bank cards, online banking systems and payment platforms, for unlawful operations.

The traditional criminal law concept of fraud is based on the idea that the victim voluntarily transfers property as a result of deception. However, in cases involving unauthorised access to electronic payment systems, the offender is more likely to interact with an automated technological system than a person.

This raises theoretical and practical questions about whether such actions should be considered fraud or theft. The main argument in favour of classifying them as theft is that automated systems cannot be deceived because they lack consciousness and the ability to form mistaken perceptions. In such cases, the offender obtains property without the owner's voluntary participation (Shkuta, 2025).

Meanwhile, another approach suggests that digital fraud may involve indirect deception, whereby the offender manipulates information systems by impersonating an authorised user or providing false authentication data. This approach reflects the transformation of economic relations, in which digital identity becomes an important property right.

The problem is both theoretical and economic. Payment fraud results in substantial financial losses for banks, payment providers and consumers alike. According to international studies, cyber-enabled financial crime incurs substantial costs for the global economy, necessitating ongoing investment in technological protection and regulatory compliance (Anderson et al., 2019).

Therefore, criminal law should move beyond traditional concepts based solely on physical interaction to consider the functional role of digital technologies in modern economic transactions.

4.3. Outdated Legal Concepts and the Need for Technologically Neutral Regulation

One significant obstacle to the effective legal regulation of electronic fraud is the use of outdated

technological terminology. In particular, the definition of 'electronic computing technology' in Article 190 of the Criminal Code of Ukraine does not reflect contemporary technological realities.

Modern fraudulent schemes often involve artificial intelligence, automated scripts, phishing platforms, deepfake technologies, malware, blockchain technologies, cloud infrastructure and decentralised financial systems. Traditional legal categories cannot always adequately describe these technologies.

From a digital economy regulatory perspective, legislation should be technologically neutral. While excessively narrow definitions may quickly become obsolete due to rapid technological development, broad but clearly formulated categories allow legal systems to adapt to new forms of criminal behaviour.

The European Union's approach demonstrates a tendency towards technologically neutral regulation. Rather than focusing on specific technologies, the Digital Services Act and the Digital Operational Resilience Act ensure the transparency, security and accountability of digital service providers (Regulation (EU) 2022/2065; Regulation (EU) 2022/2554).

Similar principles should inform the development of criminal law mechanisms designed to combat digital fraud. Regulation should not seek to describe every possible technological method of committing fraud; rather, it should establish effective legal criteria based on the social danger of the act.

4.4. Virtual Assets, Cryptocurrency Fraud and Economic Challenges

The emergence of virtual assets has created a new dimension of economic relations, while also generating new forms of fraudulent activity. Cryptocurrencies such as Bitcoin and Ethereum, as well as stablecoins, represent digital economic values that can be transferred globally without the need for traditional financial intermediaries.

However, their technological characteristics present significant challenges to criminal law enforcement. The pseudonymous nature of blockchain transactions, the absence of central control and the ability to transfer assets across jurisdictions make it difficult to identify offenders and recover illegally obtained property (Shkuta, 2024).

From an economic perspective, uncertainty surrounding the legal status of virtual assets makes the market less predictable and increases regulatory risk. To prevent money laundering, fraud, and illegal asset transfers, the financial sector must develop additional compliance mechanisms (FATF, 2021).

One of the major problems is establishing the value of virtual assets for the purposes of criminal classification. Due to significant price volatility, the value of cryptocurrency at the time of the offence

may differ substantially from its value during the subsequent investigation or judicial proceedings. This makes it difficult to determine the amount of damage caused and classify the offence according to its severity.

International practice is increasingly recognising virtual assets as objects of economic value that require legal protection. The FATF's recommendations emphasise the importance of integrating virtual asset service providers into financial monitoring and risk management systems (FATF, 2021).

Therefore, the regulation of criminal law should recognise virtual assets as a distinct form of economic value, establishing mechanisms for their seizure, preservation and evaluation.

4.5. Digital Evidence and the Transnational Nature of Electronic Fraud

Another major challenge is the collection and evaluation of digital evidence. Unlike traditional physical evidence, digital traces are characterised by volatility and the potential for rapid modification, as well as their dependence on technological infrastructures.

Investigating electronic fraud often requires analysing IP addresses, payment histories, communication records, cloud storage data and blockchain transactions. However, identifying offenders is complicated by the use of VPN services, anonymisation technologies and cross-border digital infrastructures.

Due to the transnational nature of electronic commerce, offenders, victims, payment providers and data storage locations may be situated in different jurisdictions. Consequently, effective investigations require international co-operation and mechanisms for the rapid exchange of electronic evidence.

The Budapest Convention on Cybercrime and the international co-operation mechanisms developed by Europol and UNODC both demonstrate the importance of a coordinated approach to combatting cybercrime.

According to Europol (2023), cybercriminals are increasingly combining technological tools with traditional financial schemes. These schemes include the use of intermediaries and money mules, as well as cryptocurrency conversion and complex transaction chains. These methods make financial investigations and asset recovery significantly more complicated.

Therefore, the effectiveness of combatting electronic fraud depends not only on criminal law provisions, but also on institutional capacity, technological expertise and international co-operation.

5. Discussion: Economic Consequences of Electronic Fraud for Digital Markets

Electronic fraud should not merely be considered as an individual criminal phenomenon, but also as

a factor that influences the overall development of digital markets. Fraudulent practices affect consumer behaviour, business strategies and regulatory policies.

The first major consequence is a reduction in consumer trust. Trust is a fundamental economic resource in electronic commerce, since consumers cannot evaluate sellers or products physically before completing transactions. High levels of fraud increase perceived risk, which reduces participation in online markets (Gefen et al., 2003).

The second consequence is an increase in transaction costs. Businesses are forced to invest in cybersecurity systems, authentication technologies, monitoring procedures and compliance mechanisms. These additional costs can reduce competitiveness, particularly for small and medium-sized enterprises.

The third consequence is the need for stronger regulatory institutions. In order to prevent fraudulent behaviour, digital markets require a combination of legal regulation, technological protection and economic incentives.

Thus, effective counteraction to electronic fraud should be integrated into broader digital economy policies. The protection of digital markets requires not only criminal prosecution but also the creation of reliable institutional environments that encourage innovation and secure economic interaction.

5.1. Statistical Scale and International Comparison of Economic Losses

Recent official statistics confirm the economic consequences of fraud in the digital environment. According to the FBI's Internet Crime Complaint Center (IC3), reported losses from internet crime in the United States increased from 4.2 billion USD in 2020 to 16.6 billion USD in 2024. Consequently, within a period of five years, the reported financial losses increased almost fourfold. Despite the fact that the IC3 indicator encompasses internet crime in a more extensive manner than electronic-commerce fraud alone, it furnishes a reliable macro-level measure of the expanding economic burden engendered by digitally enabled criminal conduct. The sustained upward trajectory is presented in Figure 1.

The scale of losses is also evident in consumer protection statistics. In 2024, the U.S. Federal Trade Commission reported consumer fraud losses totalling more than 12.5 billion USD, which was 25% higher than in 2023. Investment scams accounted for 5.7 billion USD, while imposter scams generated approximately 2.95 billion USD in reported losses. These figures demonstrate that the economic effects of fraud extend beyond the direct loss of property, increasing costs related to verification, cybersecurity, insurance, compliance, and dispute resolution throughout digital markets.

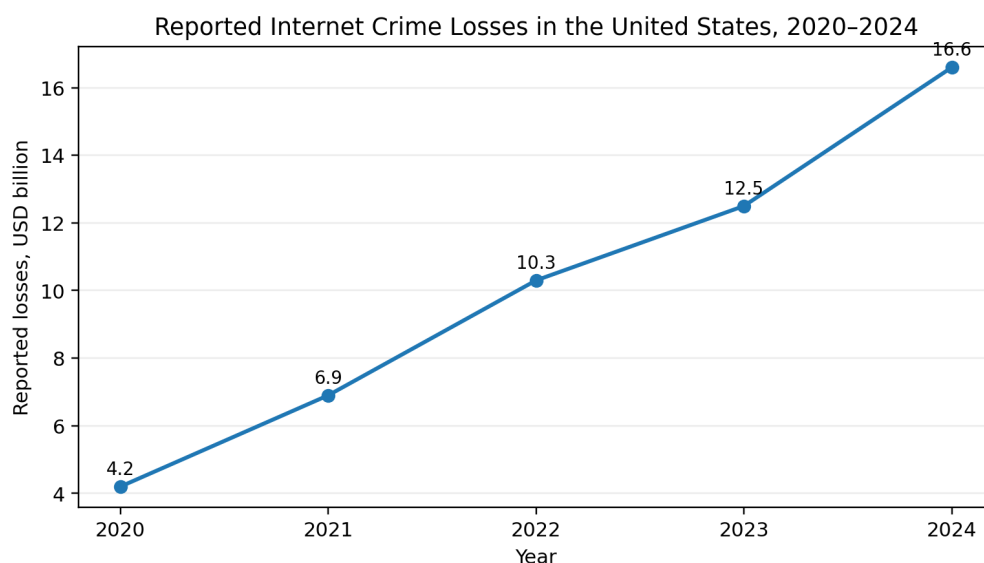


Figure 1. Reported Internet Crime Losses in the United States, 2020–2024 (billion USD)

Source: compiled by the authors on the basis of FBI IC3 data

An international comparison confirms that the problem is not confined to a single jurisdiction. However, direct comparisons require caution, as national and supranational institutions apply different reporting methodologies and cover different categories of fraudulent conduct. In the European Economic Area, the EBA and ECB have estimated that the total value of payment fraud will reach 4.2 billion EUR in 2024, up from 3.5 billion EUR in 2023. In the United Kingdom, UK Finance reported that more than 1 billion GBP was stolen through payment fraud in 2024. Unauthorised fraud alone generated losses of 722 million GBP, while losses from remote purchases approached 400 million GBP. These figures suggest that digital fraud imposes a significant economic burden on mature digital markets, even where strong authentication and advanced payment security mechanisms are widely used.

Therefore, the comparison should be interpreted as evidence of the transnational scale and economic significance of fraud, rather than as a strict ranking of jurisdictions. Differences in currencies, reporting thresholds, institutional mandates, victim reporting behaviour, and the legal classification of fraud prevent the direct comparison of absolute values. Nevertheless,

all the selected datasets indicate substantial direct losses, as well as additional indirect costs, for financial institutions, online platforms, businesses, consumers and public authorities.

6. Conclusions

The digitalisation of economic relations and the rapid expansion of electronic commerce have fundamentally transformed the mechanisms of market interaction, creating new opportunities for economic development while simultaneously generating new forms of criminal threats. Electronic fraud has become one of the most significant challenges for digital markets because it directly affects consumer confidence, business activity, and the stability of online economic relations.

The findings of the research demonstrate that the traditional criminal law model of fraud qualification is not sufficiently adapted to the characteristics of the digital environment. The absence of direct interaction between participants, the anonymity of users, the use of automated systems, the cross-border nature of transactions, and the volatility of digital evidence significantly complicate the establishment of the objective and subjective elements of fraud.

Table 1

Selected international indicators of the economic losses caused by fraud in 2024

Jurisdiction / source	Reference period	Reported losses	Scope / methodological note
United States – FBI IC3	2024	16.6 billion USD	Complaint-reported internet crime losses
United States – FTC	2024	12.5 billion USD	Consumer-reported fraud losses
European Economic Area – EBA/ECB	2024	4.2 billion EUR	Payment fraud reported by payment service providers
United Kingdom – UK Finance	2024	> 1 billion GBP	Payment fraud; includes authorised and unauthorised fraud

Source: compiled by the authors from FBI IC3, FTC, EBA/ECB and UK Finance official data

One of the key issues that remains is how to distinguish between criminal fraud and civil law violations in electronic commerce. For criminal qualification, the decisive factor should be the intention to unlawfully obtain property when receiving funds or other assets. At the same time, digital forms of interaction require clearer criteria to be developed for identifying fraudulent intent, taking into account technological characteristics and the specifics of online transactions.

The study confirms that the terminology used in criminal legislation is in need of improvement. Concepts based on outdated technological categories, such as 'electronic computing technology', do not accurately reflect the modern methods used to commit fraud. Adopting technologically neutral legal concepts related to digital technologies and computer systems would enable criminal law to respond more effectively to technological developments.

Qualifying fraudulent actions involving electronic payment systems and virtual assets remains particularly problematic. The growth of the cryptocurrency market and blockchain technology requires a unified legal

approach to recognising digital assets as objects of economic value, calculating damages and ensuring the effective seizure and recovery of illegally obtained assets.

From an economic perspective, electronic fraud has significant negative consequences for digital markets. It increases transaction costs, reduces consumer trust and forces businesses to invest additional resources in cybersecurity. It may also slow down the development of electronic commerce. Therefore, combatting digital fraud should be considered not only a task for the criminal justice system, but also an important component of digital economic policy.

Effective prevention of electronic fraud requires a comprehensive approach that combines criminal law instruments, cybersecurity mechanisms, consumer protection measures, financial monitoring systems and international co-operation. The future development of digital markets hinges on legal and economic institutions' ability to foster an environment that is both technologically innovative and secure, offering robust protection against criminal risks.

References:

- Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3), 488–500. <https://doi.org/10.2307/1879431>
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy*. Springer.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2), 213–238. <https://doi.org/10.1257/jep.29.2.213>
- Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a Financial Asset: A Systematic Analysis. *International Review of Financial Analysis*, 62, 182–199. <https://doi.org/10.1016/j.irfa.2018.09.003>
- Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation.
- FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Financial Action Task Force.
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. <https://doi.org/10.1093/rfs/hhz015>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, 27(1), 51–90.
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce. *Decision Support Systems*, 44(2), 544–564.
- Kshetri, N. (2021). *Cybercrime and Cybersecurity in the Global South*. Palgrave Macmillan.
- Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime That Is Organised? *European Journal of Crime, Criminal Law and Criminal Justice*, 25(4), 287–300.
- OECD. (2016). *Recommendation of the Council on Consumer Protection in E-commerce*. OECD Publishing.
- OECD. (2019). *Measuring the Digital Transformation: A Roadmap for the Future*. OECD Publishing.
- OECD. (2022). *The Role of Online Marketplaces in Protecting and Empowering Consumers*. OECD Publishing.
- Shkuta, O., Blaga, A., & Lisnichenko, D. (2025). Role and place of the State Bureau of investigation as a entity of preventing economic crime in the conditions of martial law in Ukraine. *Baltic Journal of Economic Studies*, 11(4), 400–404. <https://doi.org/10.30525/2256-0742/2025-11-4-400-404>
- Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3), 101–134.
- UNODC. (2021). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.
- Wall, D. S. (2017). Crime, Security and Information Communication Technologies: The Changing Cybercrime Threat. *Security Journal*, 30, 1–15.

- Williamson, O. E. (1985). *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. Free Press.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).
- Regulation (EU) 2022/2554 of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector.
- Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
- Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). 2024 IC3 Annual Report.
- Federal Trade Commission. (2025). New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024.
- European Banking Authority & European Central Bank. (2025). Joint EBA-ECB Report on Payment Fraud: 2022–2024 Data.
- UK Finance. (2025). Annual Fraud Report 2025: Fraud continues to pose a major threat with over £1 billion stolen in 2024.