IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 3, Issue: 3
2025

Cybersecurity in Financial Technologies: Civil Law Measures for Prevention and Damage Compensation

Temurbek Pulatov
Tashkent State University of Law

Abstract

The digitization of financial services has created unprecedented cybersecurity challenges requiring comprehensive civil law frameworks for prevention and damage compensation. The article examines the evolution of cybersecurity regulations in financial technology, analyzing civil law remedies and preventive measures across jurisdictions, with particular focus on Uzbekistan's emerging regulatory framework. Through comparative legal analysis and examination of recent enforcement actions, this research identifies key gaps in current civil law approaches and proposes enhanced mechanisms for cybersecurity protection in FinTech. The study reveals that while regulatory frameworks have evolved significantly, civil law remedies remain fragmented and inadequate for addressing the scale and sophistication of modern cyber threats. The research contributes to the legal scholarship by providing a comprehensive analysis of civil law measures in cybersecurity and proposing practical reforms for enhanced protection in the financial technology sector.

Keywords: Cybersecurity, Financial Technology, Civil Law, Damage Compensation, Prevention Measures, Regulatory Compliance

APA Citation:

Pulatov, T. (2025). Cybersecurity in Financial Technologies: Civil Law Measures for Prevention and Damage Compensation. *Uzbek Journal of Law and Digital Policy, 3*(3), 34–44. https://doi.org/10.59022/ujldp.338

I. Introduction

The financial technology sector has experienced unprecedented growth over the past decade, fundamentally transforming how financial services are delivered and consumed globally. This digital transformation has created new vulnerabilities and expanded the attack surface for cybercriminals, necessitating robust legal frameworks to address both prevention and remediation of cyber incidents (AllahRakha, 2024). The intersection of cybersecurity and civil law in the context of financial technologies presents unique challenges that require specialized legal approaches combining traditional civil law principles with innovative regulatory mechanisms. The significance of cybersecurity in financial services cannot be overstated. The SEC has identified information security and cybersecurity as key areas of regulation and enforcement for 2024, reflecting the growing recognition of cyber risks in financial markets. Uzbekistan faced over 11 million cyberattacks in 2023, exposing vulnerabilities and prompting the nation's first cybersecurity law, demonstrating the global nature of cyber threats and the urgent need for comprehensive legal responses.

The civil law approach to cybersecurity in financial technologies encompasses both preventive measures designed to reduce the likelihood and impact of cyber incidents, and compensatory mechanisms to address damages when breaches occur. This dual approach recognizes that while prevention is paramount, the reality of cyber threats requires effective remedial measures to ensure adequate protection for financial institutions and their customers. This study addresses the critical research question: How can civil law measures be optimized to provide effective prevention and damage compensation in the cybersecurity context of financial technologies? The research examines existing legal frameworks, analyzes their effectiveness, and proposes enhanced measures to address current gaps in protection. The analysis encompasses both developed and developing jurisdictions, with particular attention to Uzbekistan's emerging cybersecurity regulatory framework.

The methodology employed in this study combines comparative legal analysis with examination of recent enforcement actions and regulatory developments. The research draws on primary legal sources, including statutes, regulations, and case law, as well as secondary sources from legal scholarship and regulatory guidance. The analysis is informed by recent cybersecurity incidents and their legal consequences, providing practical insights into the effectiveness of current civil law measures.

The scholarly literature on cybersecurity in financial technologies has evolved significantly in recent years, reflecting the growing recognition of cyber risks as a fundamental challenge to financial stability and consumer protection. Early scholarship focused primarily on technical aspects of cybersecurity, with limited attention to legal and regulatory dimensions (Anderson et al., 2013). However, recent research has increasingly recognized the critical role of legal frameworks in addressing cybersecurity challenges.

Oyeniyi, Ugochukwu, and Mhlongo, examined the evolution of cybersecurity regulations in financial services, highlighting the shift from voluntary guidelines to mandatory compliance requirements (Oyeniyi et al., 2024). Their analysis demonstrated that regulatory frameworks have become increasingly sophisticated, incorporating risk-based approaches and emphasizing the importance of governance and oversight. This trend is evident in recent regulatory developments, including enhanced oversight and governance measures requiring covered entities' senior governing bodies to have sufficient understanding of cybersecurity-related matters. The civil law dimension of cybersecurity has received growing attention from legal scholars. Johnson analyzed the application of traditional tort principles to cybersecurity incidents, identifying challenges in establishing causation and quantifying damages in complex cyber incidents (Johnson, 2005) . Their work highlighted the need for specialized legal frameworks that can address the unique characteristics of cyber risks while maintaining consistency with established civil law principles.

Recent research has also examined the effectiveness of different regulatory approaches. Shafqat and Masood conducted a comparative analysis of cybersecurity regulations across jurisdictions, finding significant variations in approach and effectiveness. Their study identified key factors contributing to successful cybersecurity regulation, including clear standards, effective enforcement mechanisms, and appropriate penalties for non-compliance (Shafqat & Masood, 2016). The literature on damage compensation in cybersecurity incidents has highlighted the challenges of quantifying and allocating losses in complex cyber events. Burger examined the evolution of cyber insurance markets and their interaction with legal liability frameworks, identifying gaps in coverage and compensation mechanisms. Their research demonstrated the need for enhanced coordination between legal and insurance mechanisms to ensure adequate protection for affected parties (Burger, 2021).

Emerging scholarship has also examined the role of technology in legal compliance and enforcement. Kaur, Gabrijelčič and Klobučar analyzed the potential for artificial intelligence and machine learning to enhance cybersecurity compliance monitoring and enforcement (Kaur et al., 2023). Their work suggested that technological solutions could significantly improve the effectiveness of legal frameworks while reducing compliance costs. The literature on cybersecurity in developing countries has received increasing attention, particularly in the context of financial inclusion and technological leapfrogging. Narsina examined cybersecurity challenges in emerging markets, highlighting the need for tailored regulatory approaches that account for different levels of technological development and regulatory capacity (Narsina, 2022).

Despite the growing body of literature, significant gaps remain in our understanding of optimal civil law approaches to cybersecurity in financial

technologies. Limited research has examined the effectiveness of different damage compensation mechanisms, and there is insufficient analysis of how traditional civil law principles should be adapted to address cyber risks. This study aims to address these gaps by providing a comprehensive analysis of civil law measures and proposing practical reforms for enhanced protection.

II. Methodology

This study employs a mixed-methods approach combining doctrinal legal analysis with comparative case study methodology to examine civil law measures for cybersecurity in financial technologies. The research design was selected to provide both depth and breadth of analysis, allowing for detailed examination of specific legal frameworks while maintaining comparative perspective across jurisdictions. The doctrinal analysis component examines primary legal sources including statutes, regulations, and judicial decisions related to cybersecurity in financial services. This analysis focuses on identifying key legal principles, examining their application in practice, and assessing their effectiveness in addressing cybersecurity challenges. The research draws on legal databases including Westlaw, LexisNexis, and jurisdiction-specific legal databases to ensure comprehensive coverage of relevant legal materials.

The comparative case study methodology examines cybersecurity regulatory frameworks across multiple jurisdictions, with particular focus on the United States, European Union, and Uzbekistan. This approach allows for identification of best practices and common challenges while accounting for differences in legal systems and regulatory approaches. The selection of jurisdictions was based on their significance in global financial markets, the sophistication of their cybersecurity regulatory frameworks, and their relevance to the research questions.Data collection for this study involved systematic review of legal materials, regulatory guidance, and enforcement actions related to cybersecurity in financial services.

The research examined recent developments in cybersecurity regulation, including new requirements for governance and oversight, enhanced disclosure obligations, and expanded enforcement actions. Particular attention was paid to civil law remedies and damage compensation mechanisms. The analysis of Uzbekistan's cybersecurity framework was based on examination of the Law "On Cybersecurity" (No. ORQ-764 dated 15 April 2022) which came into force on July 17, 2022, as well as subsequent regulatory developments and enforcement actions. The research also examined Presidential Resolution No. PP-167 dated May 31, 2023 on additional measures to improve the system of cybersecurity of critical information infrastructure facilities.

The study's methodology incorporates both quantitative and qualitative analytical approaches. Quantitative analysis examined trends in cybersecurity incidents, enforcement actions, and financial penalties to identify patterns and assess the effectiveness of different regulatory approaches. The research noted that the SEC

obtained orders for $8.2 billion in financial remedies in fiscal year 2024, the highest amount in agency history, indicating the scale of cybersecurity-related enforcement actions. Qualitative analysis focused on examining the substantive content of legal frameworks, identifying gaps and inconsistencies, and assessing the adequacy of current civil law measures. This analysis drew on legal scholarship, regulatory guidance, and industry best practices to develop recommendations for enhanced protection.

The research methodology also incorporated examination of recent cybersecurity incidents and their legal consequences to provide practical insights into the effectiveness of current civil law measures. This approach allowed for assessment of how legal frameworks perform in practice and identification of areas requiring reform. Limitations of this methodology include the rapidly evolving nature of cybersecurity threats and regulations, which may affect the currency of certain findings. Additionally, the comparative analysis is limited by differences in legal systems and regulatory approaches, which may affect the generalizability of findings across jurisdictions.

III. Results

A. Current Regulatory Landscape

The analysis reveals a rapidly evolving regulatory landscape for cybersecurity in financial technologies, characterized by increasing sophistication and enforcement activity. The SEC and Commodity Futures Trading Commission both imposed record-high financial remedies in their 2024 fiscal year, while bringing substantially fewer enforcement actions than in recent years, indicating a shift toward more targeted but impactful enforcement actions. Regulatory frameworks have evolved to address emerging threats and technological developments. PSD3 introduces significant changes for banks and non-bank payment service providers, including new Strong Customer Authentication regulations with stricter rules around data access, payment protection, and authentication of users.

This evolution reflects the growing recognition of the need for comprehensive regulatory approaches that address both technical and legal dimensions of cybersecurity. The research identified significant variations in regulatory approaches across jurisdictions. While some jurisdictions have adopted comprehensive frameworks covering all aspects of cybersecurity, others have focused on specific areas such as data protection or incident reporting. This fragmented approach creates challenges for multinational financial institutions and may create regulatory arbitrage opportunities.

B. Civil Law Measures for Prevention

The analysis of preventive civil law measures reveals several key approaches currently employed across jurisdictions. Regulatory frameworks increasingly

emphasize governance and oversight requirements, with enhanced oversight and governance measures requiring covered entities' senior governing bodies to have sufficient understanding of cybersecurity-related matters to exercise effective oversight. Compliance obligations have become more detailed and prescriptive, with specific requirements for risk assessment, incident response planning, and third-party risk management. The research found that effective preventive measures typically include:

Governance and Oversight Requirements-modern regulatory frameworks emphasize the importance of board-level oversight of cybersecurity risks. This includes requirements for cybersecurity expertise on boards, regular reporting on cybersecurity risks, and integration of cybersecurity considerations into strategic planning processes. Risk Assessment and Management-regulatory frameworks increasingly require comprehensive risk assessment processes that identify, assess, and prioritize cybersecurity risks. These requirements often include specific methodologies for risk assessment and regular updating of risk assessments to reflect changing threats.

Incident Response Planning-preventive measures include requirements for comprehensive incident response plans that address detection, containment, eradication, and recovery from cyber incidents. These plans must be regularly tested and updated to ensure effectiveness. Third-Party Risk Management-given the interconnected nature of financial services, regulatory frameworks increasingly address third-party risks, requiring due diligence on vendors and service providers, contractual provisions addressing cybersecurity, and ongoing monitoring of third-party risks. Employee training and awareness-preventive measures include requirements for cybersecurity training and awareness programs for employees, recognizing that human factors are often critical in cybersecurity incidents.

C. Damage Compensation Mechanisms

The analysis of damage compensation mechanisms reveals significant gaps and inconsistencies in current approaches. While regulatory frameworks have evolved to address prevention, compensation mechanisms remain fragmented and often inadequate to address the full scope of damages from cyber incidents. Regulatory authorities have significantly increased the use of monetary penalties for cybersecurity violations. However, these penalties are typically paid to regulatory authorities rather than compensating affected parties. Some jurisdictions provide private rights of action for cybersecurity-related damages, but these are often limited in scope and may not cover all types of damages. Cyber insurance has emerged as an important component of damage compensation, but coverage gaps and exclusions limit its effectiveness. Some regulatory frameworks provide for restitution to affected parties, but these mechanisms are not consistently applied across jurisdictions.

D. Uzbekistan's Cybersecurity Framework

The analysis of Uzbekistan's cybersecurity framework reveals a rapidly developing regulatory environment responding to significant cyber threats. Uzbekistan faced over 11 million cyberattacks in 2023, exposing vulnerabilities and prompting the nation's first cybersecurity law. The scale of the challenge is further evidenced by the fact that in 2024, 44.4% of all crimes were cyber-related, with malicious software and links accounting for 60% of attacks, granting unauthorized access to financial information. Uzbekistan adopted its first Law "On Cybersecurity" (No. ORQ-764 dated 15 April 2022) which came into force on July 17, 2022. This foundational legislation established the basic framework for cybersecurity regulation in the country. Subsequently, Presidential Resolution No. PP-167 dated May 31, 2023 endorsed additional measures to improve the system of cybersecurity of critical information infrastructure facilities.

The framework has continued to evolve, with Presidential Decree No PQ-153 dated 30 April 2025 aimed at bolstering cybersecurity measures and targeting cybercrimes across the country. This ongoing development reflects the dynamic nature of cyber threats and the need for adaptive regulatory responses. The framework addresses cybersecurity across all sectors, with particular attention to critical infrastructure and financial services. The law establishes clear institutional responsibilities for cybersecurity oversight and coordination. The framework imposes specific obligations on organizations, including risk assessment, incident reporting, and security measures implementation. The framework provides for both administrative and criminal penalties for cybersecurity violations.

However, the analysis also identified several areas where Uzbekistan's framework could be strengthened. The current framework focuses primarily on administrative and criminal penalties, with limited provision for civil law remedies and damage compensation. While the framework addresses compliance obligations, there is limited provision for private sector participation in cybersecurity governance. The framework could benefit from enhanced mechanisms for international coordination and information sharing.

IV. Discussion

A. Gaps in Current Civil Law Approaches

The analysis reveals several critical gaps in current civil law approaches to cybersecurity in financial technologies. These gaps create vulnerabilities that can be exploited by cybercriminals and may leave affected parties without adequate recourse when incidents occur. The most significant gap identified is the fragmented nature of damage compensation mechanisms. While regulatory frameworks have evolved to address prevention and enforcement, compensation mechanisms remain poorly coordinated and often inadequate. This creates a situation where organizations may face significant regulatory penalties while affected parties receive limited compensation for their losses.

Another critical gap is the limited integration of cybersecurity considerations into traditional civil law frameworks. Contract law, tort law, and other areas of civil law have not adequately adapted to address the unique characteristics of cyber risks. This creates uncertainty about legal obligations and remedies in cyber incidents, potentially undermining the effectiveness of legal protections. The cross-border nature of cyber threats creates additional challenges for civil law frameworks. Traditional civil law mechanisms are designed for domestic disputes and may not be well-suited to address incidents that span multiple jurisdictions. This creates opportunities for regulatory arbitrage and may limit the effectiveness of legal remedies.

Based on the analysis, several enhancements to civil law measures are proposed to address identified gaps and improve the effectiveness of cybersecurity protection in financial technologies. The research proposes the development of comprehensive damage compensation mechanisms that address the full scope of losses from cyber incidents. This would include direct financial losses, business interruption costs, reputation damage, and costs of remediation and recovery. The mechanism should provide for both individual and collective redress, recognizing that cyber incidents often affect multiple parties. The complexity of cyber incidents and the specialized knowledge required to address them suggest the need for specialized judicial mechanisms. Cyber courts with expertise in technology and cybersecurity could provide more effective resolution of cyber-related disputes and ensure consistent application of legal principles.

The research suggests consideration of mandatory cyber insurance requirements for financial institutions above a certain size or systemic importance. This would help ensure adequate resources are available for damage compensation while creating market incentives for improved cybersecurity practices. Given the cross-border nature of cyber threats, enhanced international coordination mechanisms are essential. This could include mutual legal assistance treaties specifically addressing cyber incidents, standardized incident reporting across jurisdictions, and coordinated enforcement actions. The rapid pace of technological change requires regulatory frameworks that can adapt quickly to new threats and technologies. This could include regulatory sandboxes for new technologies, fast-track processes for updating regulations, and delegation of detailed technical requirements to specialized agencies.

B. Implications for Uzbekistan's Framework

The analysis has specific implications for Uzbekistan's developing cybersecurity framework. While the country has made significant progress in establishing a foundational regulatory framework, several areas require further development to ensure comprehensive protection. The most critical need is for enhanced civil law remedies and damage compensation mechanisms. The current framework focuses primarily on administrative and criminal penalties, with limited provision for civil remedies. This gap should be addressed through development of comprehensive civil law provisions that provide adequate remedies for affected parties. Uzbekistan should

also consider enhanced private sector engagement in cybersecurity governance.

While the current framework addresses compliance obligations, there is limited provision for private sector participation in policy development and implementation. This could be addressed through establishment of public-private partnerships and industry advisory bodies. International coordination is another area requiring attention. As cyber threats are global in nature, Uzbekistan's cybersecurity framework should include robust mechanisms for international coordination and information sharing. This could include participation in international cybersecurity organizations and development of bilateral cooperation agreements. The rapid growth of Uzbekistan's digital economy, including the establishment of International Digital Technology Center with special attractive legal regime for foreign companies, creates additional urgency for comprehensive cybersecurity protections. The framework should be designed to support innovation while ensuring adequate protection against cyber threats.

Conclusion

This study has examined civil law measures for prevention and damage compensation in cybersecurity for financial technologies, with particular focus on Uzbekistan's emerging regulatory framework. The analysis reveals a rapidly evolving regulatory landscape characterized by increasing sophistication and enforcement activity, but also significant gaps in current approaches. The research demonstrates that while preventive measures have become more comprehensive and sophisticated, damage compensation mechanisms remain fragmented and often inadequate. This creates a situation where organizations may face significant regulatory penalties while affected parties receive limited compensation for their losses. The cross-border nature of cyber threats further complicates the application of traditional civil law mechanisms.

The analysis of Uzbekistan's cybersecurity framework reveals significant progress in establishing foundational regulations, but also identifies areas requiring further development. The country's experience with large-scale cyber threats has prompted rapid regulatory development, but gaps remain in civil law remedies and damage compensation mechanisms. The study proposes several enhancements to civil law measures, including comprehensive damage compensation mechanisms, specialized cyber courts, mandatory cyber insurance, enhanced international coordination, and adaptive regulatory frameworks. These proposals address identified gaps while building on the strengths of existing approaches.

For Uzbekistan specifically, the research recommends development of enhanced civil law remedies, increased private sector engagement, and strengthened international coordination mechanisms. These developments would support the country's growing digital economy while ensuring adequate protection against cyber threats. The findings of this study contribute to the growing body of legal scholarship

on cybersecurity by providing comprehensive analysis of civil law measures and proposing practical reforms. The research demonstrates the need for continued evolution of legal frameworks to address emerging challenges while maintaining fundamental principles of civil law.

The study's implications extend beyond academic scholarship to practical policy development. The proposed enhancements to civil law measures could inform regulatory reform efforts in multiple jurisdictions, while the analysis of Uzbekistan's framework provides insights relevant to other developing countries facing similar challenges. Future research should focus on empirical assessment of damage compensation mechanism effectiveness, comparative analysis of developing country frameworks, and examination of emerging technologies' impact on cybersecurity law. Such research would further enhance understanding of optimal approaches to cybersecurity protection in financial technologies.

It emphasizes that effective cybersecurity protection requires comprehensive legal frameworks that address both prevention and remediation. While significant progress has been made in developing such frameworks, continued evolution is necessary to address emerging challenges and ensure adequate protection for all stakeholders in the financial technology ecosystem. The study's findings underscore the critical importance of cybersecurity in financial technologies and the need for robust legal frameworks to address associated risks. As the digital transformation of financial services continues, the development of effective civil law measures for cybersecurity protection will remain a priority for policymakers, regulators, and legal scholars alike.

Bibliography

AllahRakha, N. (2024). Transformation of crimes (cybercrimes) in digital age. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.156

AllahRakha, N. (2024). UNESCO's AI ethics principles: Challenges and opportunities. *International Journal of Law and Policy*, *2*(9), 24–36. https://doi.org/10.59022/ijlp.225

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *Springer eBooks* (pp. 265–300). https://doi.org/10.1007/978-3-642-39498-0_12

Burger, E. S. (2021). Professional responsibility, legal malpractice, cybersecurity, and cyber-insurance in the COVID-19 era. *St. Mary's Journal on Legal Malpractice & Ethics*, *11*(2), 234–275. https://commons.stmarytx.edu/lmej/vol11/iss2/2

Johnson, V. R. (2005). Cybersecurity, identity theft, and the limits of tort liability. *South Carolina Law Review*, *57*, 255–294.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, Article 101804. https://doi.org/10.1016/j.inffus.2023.101804

Law "On Cybersecurity" of the Republic of Uzbekistan, No. ORQ-764 (2022).

Narsina, D. (2022). Impact of cybersecurity threats on emerging markets' integration into global trade networks. *American Journal of Trade and Policy*, *9*(3), 141–148. https://doi.org/10.18034/ajtp.v9i3.741

Oyeniyi, N. L. D., Ugochukwu, N. C. E., & Mhlongo, N. N. Z. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. *Computer Science & IT Research Journal*, *5*(4), 903–925. https://doi.org/10.51594/csitrj.v5i4.1049

Presidential Decree of the Republic of Uzbekistan, No. PQ-153 (2025).

Presidential Resolution of the Republic of Uzbekistan, No. PP-167 (2023).

Securities and Exchange Commission. (2024). *SEC announces enforcement results for fiscal year 2024*. https://www.sec.gov/newsroom/press-releases/2024-186

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129–136. https://www.scirp.org/reference/referencespapers?referenceid=3828262

U.S. Department of the Treasury, Office of the Comptroller of the Currency. (2024). *Cybersecurity and financial system resilience report 2024*. OCC.