INTERNATIONAL CONFERENCE ON THE STATE, LAW, POLITICS & DEMOCRACY (ICON-SLPD)
P-ISSN : 2962-7109 E-ISSN : 3063-6957
https://openjournal.unpam.ac.id/index.php/ICon

International Conference On The State, Law, Politics & Democracy (ICON-SLPD)
Conference Proceedings 2025

Addressing Criminal Liability in the Abuse of Financial Technology and Digital Assets: Empirical Evidence on Consumer Protection in Yogyakarta

Neva Sari Susanti[1], Elvira[2], Anggit Hanjani[3]

[a]Faculty of Law, University Pamulang, Tangsel, E-mail: dosen02788@unpam.ac.id
[b]Faculty of Law, University Pamulang, Tangsel, E-mail: dosen02660@unpam.ac.id
[c]Faculty of Law, University Pamulang, Tangsel, E-mail: enenganggit55@gmail.com

Article

Received: Des 02, 2025;
Reviewed: Jan 07, 2026;
Accepted: Feb 09, 2026;
Published: Feb 26, 2026

Abstract

The rapid development of financial technology (fintech) and digital assets has significantly transformed financial services, while simultaneously increasing the risk of misuse that may harm consumers. In Indonesia, the regulatory framework governing fintech and digital assets continues to evolve, yet challenges remain in ensuring effective criminal liability and consumer protection. This study aims to examine the implementation of criminal liability in cases involving the abuse of fintech and digital assets and to assess its effectiveness in protecting consumers, with a limited empirical focus on Yogyakarta. This research employs a normative-empirical legal research method. The normative approach analyzes statutory regulations related to fintech, digital assets, consumer protection, and criminal law, including financial services and electronic transaction regulations. The empirical approach is conducted through interviews and field observations involving law enforcement officials, regulators, fintech practitioners, and affected consumers in Yogyakarta to capture practical challenges in law enforcement and regulatory implementation.The findings indicate that the application of criminal liability in fintech and digital asset abuse cases faces several obstacles, including regulatory gaps, overlapping institutional authority, limited technical capacity of law enforcement agencies, and low public legal awareness. These challenges weaken deterrence and reduce the effectiveness of consumer protection mechanisms. The study further reveals that existing legal instruments have not been optimally integrated to address the complex nature of digital financial crimes. This research concludes that strengthening criminal liability requires regulatory harmonization, improved inter-agency coordination, and enhanced institutional capacity, alongside preventive measures such as consumer education and compliance-based regulation. The study contributes to the development of evidence-based legal policy recommendations aimed at improving consumer protection in the digital financial ecosystem.

Keywords: criminal liability, financial technology, digital assets, consumer protection, fintech abuse, Indonesia.

A. INTRODUCTION

The rapid expansion of financial technology (fintech) and digital assets has fundamentally reshaped the global financial services landscape, transforming how consumers access credit, conduct transactions, and participate in investment activities. Digital innovations such as peer-to-peer lending platforms, electronic payment systems, and crypto-assets have significantly improved financial inclusion and operational efficiency. However, these advancements have simultaneously generated new legal risks, including fraud, misuse of personal data, illegal lending practices, and unlicensed digital asset trading. The velocity of innovation in digital finance frequently outpaces the capacity of legal systems to adapt, resulting in regulatory gaps and weakened consumer protection.

In Indonesia, the governance of fintech and digital assets is regulated through a combination of sectoral regulations issued by financial authorities, electronic transaction laws, consumer protection statutes, and data protection legislation. Despite this regulatory development, enforcement remains largely administrative and preventive. Criminal law intervention essential for deterrence and accountability has not been systematically integrated into the digital finance regulatory framework. Consequently, the attribution of criminal liability for abuses involving fintech platforms and digital assets remains fragmented, inconsistent, and legally uncertain.

Empirical evidence at the national level underscores the urgency of this issue. According to reports from the Indonesian Financial Services Authority (OJK) covering the period 2022–2024, consumer complaints reached 39,866 cases, with fintech lending and digital asset trading consistently ranking among the top three sources of complaints nationwide (1). During the same period, more than 1,300 illegal fintech entities and over 500 unregistered crypto-assets were blocked by the Illegal Financial Activities Task Force (Satgas PASTI) (2). These figures reflect a systemic imbalance between rapid digital innovation and insufficient criminal law protection for consumers.

Yogyakarta represents a particularly relevant empirical context for examining this imbalance. The region's heterogeneous social structure characterized by a strong academic population, a vibrant small and medium enterprise (SME) sector, and a substantial low-income community makes it a representative microcosm of Indonesia's digital economy. Many SMEs in Yogyakarta rely on fintech services for financing and payment systems but lack adequate legal literacy when confronted with default risks, fraud, or misuse of personal data. Simultaneously, Yogyakarta has emerged as an active hub for digital asset users, particularly among students and young retail investors, who are frequently exposed to high-risk and misleading investment schemes.

Empirical developments in Yogyakarta between 2022 and 2024 reveal several recurring patterns: (i) a sharp increase in complaints related to illegal online lending and unethical debt collection involving intimidation and dissemination of personal data; (ii) widespread misuse of personal data in digital transactions, particularly by unlicensed fintech operators; (iii) the proliferation of unregistered crypto investment schemes exploiting regulatory ambiguity; and (iv) weak coordination among law enforcement agencies, resulting in many cases being resolved administratively or through mediation rather than criminal prosecution (3–6).

These conditions reveal a significant normative–empirical gap. Normatively, Indonesia has enacted key regulations such as OJK Regulation No. 6/POJK.07/2022 on Consumer Protection and Law No. 27 of 2022 on Personal Data Protection. Empirically, however, violations that substantively fulfill the elements of criminal offenses such as fraud, extortion, and illegal access to electronic data are rarely pursued through criminal justice mechanisms.

This enforcement gap undermines legal certainty, weakens deterrence, and erodes public trust in digital financial services.

PROBLEM STATEMENT

Against this background, this study addresses the central problem of how criminal liability is conceptualized and enforced in cases involving the abuse of fintech services and digital assets that harm consumers. It examines why violations with clear criminal elements are often excluded from criminal proceedings, how enforcement practices diverge from normative legal frameworks, and what legal and institutional reforms are necessary to strengthen consumer protection. By employing a normative empirical approach with a limited empirical focus on Yogyakarta, this research aims to provide evidence-based recommendations for integrating criminal liability into Indonesia's digital finance governance framework while maintaining legal certainty and supporting sustainable innovation.

B. MATERIALS AND METHODS

This study employs a qualitative socio-legal methodology combined with action research. The socio-legal approach is used to analyze legal norms and governance structures regulating Smart Living implementation, while action research enables real-time policy testing and improvements in collaboration with stakeholders.

2.1 Study Location

This study was conducted in the Special Region of Yogyakarta, Indonesia. Yogyakarta was selected as the study location due to its unique socio-economic characteristics that reflect Indonesia's broader digital finance ecosystem. The region hosts a heterogeneous population comprising university students, small and medium enterprise (SME) actors, digital platform users, and informal sector workers, all of whom actively engage with financial technology services and digital asset platforms. Moreover, Yogyakarta has experienced a notable increase in consumer complaints related to fintech lending and digital asset investments between 2022 and 2024, making it a suitable empirical setting to examine the effectiveness of criminal liability in protecting consumers within the digital financial sector.

2.2 Data Collection

This research employed a mixed normative–empirical approach. Normative legal data were collected through systematic analysis of statutory instruments, including Law No. 8 of 1999 on Consumer Protection, Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions, Law No. 27 of 2022 on Personal Data Protection, OJK Regulation No. 6/POJK.07/2022, and relevant criminal law provisions under the Indonesian Penal Code.

Empirical data were obtained through semi-structured interviews and document review. Interviews were conducted with key informants, including: (i) consumer protection officials at the Regional OJK Office (n = 4); (ii) law enforcement officers handling cybercrime and financial crimes (n = 5); (iii) fintech compliance officers and legal consultants (n = 4); (iv) consumer advocacy representatives (n = 3); and (v) affected consumers, including SME actors and individual digital asset users (n = 10). Supporting documents, such as complaint records, enforcement reports, and publicly available regulatory announcements, were also examined to triangulate interview findings.

2.3 Action Research Protocol

This study adopted an action research protocol to ensure policy relevance and practical applicability. The protocol consisted of four iterative stages: (1) problem diagnosis through identification of recurring patterns of digital financial abuse and enforcement gaps; (2) reflective analysis by comparing empirical findings with existing criminal and regulatory frameworks; (3) model formulation through the development of a criminal liability integration framework for fintech and digital asset regulation; and (4) validation through focused group discussions (FGDs) involving regulators, legal practitioners, and consumer representatives. This cyclical approach enabled continuous refinement of legal recommendations based on stakeholder feedback and empirical realities.

2.4 Data Analysis

Normative data were analyzed using doctrinal legal analysis, focusing on statutory interpretation, legal consistency, and liability construction. Empirical data from interviews were transcribed verbatim and analyzed using qualitative thematic analysis. Coding was conducted inductively to identify recurring themes related to enforcement practices, institutional coordination, and barriers to criminal prosecution. The findings from normative and empirical analyses were then integrated using a triangulation technique to map divergences between legal norms and enforcement practices and to formulate evidence-based policy recommendations.

2.5 Data Availability Statement

The qualitative datasets generated and analyzed during the current study are not publicly available due to confidentiality and ethical considerations, particularly the protection of informant identities and sensitive enforcement information. However, anonymized data excerpts and regulatory materials supporting the findings of this study are available from the corresponding author upon reasonable request.

2.6 Replicability Commitment

To ensure replicability and methodological transparency, this study provides a detailed description of data sources, interview protocols, analytical procedures, and legal materials examined. Future researchers may replicate this study by applying the same normative–empirical framework, interview guidelines, and analytical methods in other regions or jurisdictions to assess the generalizability of findings related to criminal liability in digital finance governance.

C. RESULT AND DISCUSSION

3.1 Overview of Consumer Complaints in Yogyakarta

Analysis of consumer complaint data from 2022–2024 highlights a growing pattern of abuse in the digital financial sector. A total of 39,866 consumer complaints were recorded nationally, with fintech lending and digital asset platforms among the top three sources of grievances. In Yogyakarta, interviews and document review revealed that approximately 40% of complaints involved illegal lending practices, improper debt collection, or unlicensed digital asset transactions. The data indicate a systemic gap between regulatory expectations and practical enforcement, consistent with national trends (1,2,5)

3.2 Legal and Regulatory Gaps

Normative analysis revealed significant gaps in the application of criminal liability for fintech and digital asset abuses. While Law No. 8/1999 on Consumer Protection, Law No.

11/2008 (amended), and Law No. 27/2022 on Personal Data Protection provide a framework for consumer rights, enforcement often defaults to administrative measures or mediation. Interviews with law enforcement officers (n=5) and OJK officials (n=4) highlighted procedural ambiguities and institutional fragmentation as major obstacles preventing criminal prosecution of offenses such as fraud, illegal data access, and coercive collection practices.

This gap reflects a disharmony between existing legal frameworks and real-world practice**,** emphasizing the need for integrative legal mechanisms that combine regulatory oversight, criminal liability, and stakeholder empowerment

3.3 Empirical Findings: Key Patterns

Three main patterns emerged from the empirical data:

1. High vulnerability of SMEs and individual users . Many SME actors and individual consumers lack awareness of legal remedies and face challenges navigating digital finance contracts (3,7,9).
2. Prevalence of unlicensed operators. More than 1,300 illegal fintech entities **and** 500 unregistered crypto platforms were blocked by Satgas PASTI as of mid-2024, yet many continue operating through informal channels, highlighting enforcement limitations (4,6,8).
3. Weak institutional coordination. Fragmentation among OJK, law enforcement, and consumer advocacy bodies reduces the effectiveness of criminal prosecution, often resulting in administrative or civil resolution only (10,11).

3.4 Integrative Approach to Criminal Liability

The study proposes a normative-empirical integrative model that aligns with both regulatory expectations and ground realities:

- Criminal Accountability Layer: Applying targeted criminal sanctions for fraud, illegal collection, and unauthorized access to consumer data.
- Preventive Regulatory Measures: Strengthening licensing, monitoring, and reporting obligations for fintech and digital asset platforms.
- Consumer Empowerment: Educating users on rights and legal remedies, supported by simplified complaint mechanisms.

Focus group discussions (FGDs) confirmed the feasibility of such a model in Yogyakarta, emphasizing that integration of legal sanctions with consumer empowerment and regulatory oversight enhances both compliance and trust.

3.5 Policy Implications

The findings indicate that criminal liability for fintech and digital asset abuse is underutilized, reducing deterrence effects and consumer protection. Recommendations include:

1. Harmonizing criminal and administrative provisions to facilitate enforcement.
2. Enhancing coordination between OJK, law enforcement, and consumer advocacy agencies.
3. Implementing awareness campaigns targeting high-risk users, particularly SMEs and youth investors.

4. Establishing pilot programs to test integrative enforcement models, which can later be scaled nationally.

This approach aligns with ASTA CITA objectives and SDG goals on inclusive economic growth, reduced inequalities, and strengthened institutions by ensuring consumers are protected in digital markets (12–15).

3.6 Discussion

The combination of normative-empirical evidence highlights the critical gap between legal frameworks and enforcement practices. The escalation of unlicensed fintech and digital asset activities in Yogyakarta demonstrates the need for criminal liability as a complementary tool to regulatory oversight. Findings confirm that legal harmonization, institutional collaboration, and stakeholder engagement are essential for adaptive and responsive policy-making, consistent with international best practices in consumer protection and digital finance governance (16–20).

D. CONCLUSION

4.1 Conclusion

This study demonstrates that the current regulatory approach to fintech and digital assets in Indonesia remains insufficient to ensure effective consumer protection when criminal violations occur. While administrative and preventive regulations have expanded, criminal law enforcement has not kept pace with the complexity and scale of digital financial abuses. The findings confirm a substantial gap between normative legal provisions and empirical enforcement practices, particularly in the attribution of criminal liability to fintech operators and digital asset service providers. As evidenced by the Yogyakarta case, this gap results in under-deterrence, limited victim redress, and declining public trust in digital financial systems.

4.2 Policy Recommendations

Based on these findings, this study proposes the following policy recommendations:

1. **Integration of Criminal Liability into Fintech Regulation**
   Criminal law provisions should be explicitly integrated into fintech and digital asset regulations to clarify offense classifications, liability standards, and enforcement procedures.
2. **Strengthening Inter-Agency Coordination**
   Formal coordination mechanisms among financial regulators, cybercrime units, prosecutors, and consumer protection agencies are essential to ensure consistent criminal law enforcement.
3. **Clear Standards for Corporate Criminal Liability**
   Legal frameworks should define corporate criminal responsibility for fintech operators, including vicarious liability and compliance-based defenses.
4. **Enhanced Data Protection Enforcement**
   Criminal sanctions for severe personal data misuse should be operationalized to complement administrative penalties under data protection law.
5. **Consumer-Centered Legal Literacy Programs**
   Targeted legal education initiatives for SMEs, students, and retail investors are necessary to reduce vulnerability and improve reporting of digital financial crimes.

By implementing these reforms, Indonesia can develop a more coherent, deterrent-based, and consumer-oriented legal framework that balances innovation, accountability, and public trust in the digital financial ecosystem.

REFERENCES

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation*. Oxford University Press.

Bank Indonesia. (2024). *Payment system and digital finance development*. Bank Indonesia.

Black, J. (2019). Risk-based regulation and consumer protection. *Modern Law Review*.

Finck, M. (2019). *Blockchain regulation and governance*. Cambridge University Press.

Gunningham, N. (2017). *Regulatory theory: Foundations and applications*. Oxford University Press.

Indonesian National Police. (2023). *Annual cybercrime report*. Jakarta: INP.

Koops, B. J. (2010). The trouble with technology-neutral regulation. *Law, Innovation and Technology*.

Law No. 8 of 1999 on Consumer Protection.

Law No. 11 of 2008 on Electronic Information and Transactions (as amended).

Law No. 27 of 2022 on Personal Data Protection.

Lessig, L. (2006). *Code and other laws of cyberspace*. Basic Books.

Ministry of Communication and Informatics. (2023). *Digital economy and data protection report*. Jakarta: Kominfo.

OECD. (2021). *Consumer policy and fraud in digital markets*. Paris: OECD.

Otoritas Jasa Keuangan. (2023). *Fintech lending statistics*. Jakarta: OJK.

Otoritas Jasa Keuangan. (2024). *Laporan perlindungan konsumen sektor jasa keuangan 2022–2024*. Jakarta: OJK.

Otoritas Jasa Keuangan. (2022). *OJK Regulation No. 6/POJK.07/2022 on consumer protection*. Jakarta: OJK.

Polinsky, A., & Shavell, S. (2000). The economic theory of public enforcement. *Journal of Economic Literature*.

Satgas PASTI. (2024). *Siaran pers penindakan fintech dan aset kripto ilegal*. Jakarta.

UNCTAD. (2022). *Digital economy report*. Geneva: UNCTAD.

World Bank. (2020). *Consumer protection in digital financial services*. Washington, DC: World Bank.