Volume 3, No. 12 December 2025
p-ISSN 3032-3037| e-ISSN 3031-

ADVANCES IN SOCIAL HUMANITIES RESEARCH

Strengthening Law Enforcement Against Digital Identity Abuse in Online Lending: A Normative and Forensic Analysis to Achieve Legal Certainty in Indonesia

Afif Rachmat Hidayat*, Abdul Latif, Kristiawanto
Universitas Jayabaya Jakarta, Indonesia
Emails: afifrachmathdyt@gmail.com*, prof.abdul.latif59@gmail.com, drkristiawantopartners@gmail.com

Abstract
The rapid expansion of digital financial services has transformed online lending into a mainstream financial solution, yet it has simultaneously created significant vulnerabilities, particularly the misuse of digital identities. This study critically examines the legal enforcement mechanisms applied to perpetrators who unlawfully use another person's identity to obtain online loans within Indonesia's evolving cybercrime landscape. Employing a normative juridical method integrated with statutory, conceptual, and case-based approaches, this research analyzes the adequacy of existing regulations—including the Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and the Personal Data Protection Law (PDP Law)—and their practical implementation. Findings reveal that regulatory fragmentation, insufficient digital verification standards, and limited digital forensic competence hinder effective prosecution. Case analysis further demonstrates recurring challenges in evidentiary quality, particularly concerning metadata integrity, digital traceability, and chain-of-custody compliance. These constraints contribute to legal uncertainty in determining liability, thereby undermining broader legal certainty within the digital financial ecosystem. The study concludes that strengthening legal enforcement requires a multi-dimensional strategy. This includes the adoption of specialized legislation on digital identity misuse, enhancement of forensic capabilities, mandatory biometric verification for fintech providers, and integrated inter-agency coordination through a national digital identity framework. This research contributes theoretically by advancing the discourse on cybercrime and digital identity governance, and practically by offering concrete policy recommendations to enhance legal certainty, accountability, and public trust.

Keywords: Cybercrime enforcement; Digital forensics; Digital identity misuse; Legal certainty; Online lending.

Introduction

In the current era of digital civilization, human identity is no longer limited to physical existence. It now encompasses a virtual representation tied to personal data, electronic footprints, and financial activities connected to a global digital system (Pakpahan, 2021; Wibowo et al., 2023; Zen Munawar et al., 2022). Philosophically,

identity has shifted from being the core of human existence to becoming a valuable asset within the financial technology ecosystem (Risdiany et al., 2024; Trisilowati, 2017). As identity is reduced to numerical data, digital documents, and biometrics, the risks of manipulation and exploitation increase significantly. This creates a modern paradox: the convenience of financial access is accompanied by the threat of identity abuse, particularly in online lending, which presents a new form of non-physical yet highly destructive crime (Arkaan Daffa & Sidi Ahyar Wiraguna, 2025; Ekayani et al., 2023; Siti Maesaroh, 2025).

The legal framework in Indonesia, particularly Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), explicitly prohibits the unlawful use of another person's personal data, including for obtaining online loans. Perpetrators can be subject to imprisonment for up to 5 years and/or a fine of up to IDR 5 billion under Article 65(3) in conjunction with Article 67(3). If identity falsification is involved, the penalty increases to 6 years imprisonment and/or a fine of IDR 6 billion under Article 66 in conjunction with Article 68. Furthermore, online lending operators, as data controllers, are required to obtain explicit and legitimate consent from data subjects before processing personal data, in accordance with Article 20(2)(a) of the PDP Law. Violations can result in administrative sanctions. Beyond criminal and administrative sanctions, victims also retain the right to file civil lawsuits for compensation, as regulated under Article 12(1) of the PDP Law and Article 26(2) of the ITE Law. Thus, although online lending carries risks of non-physical crime, existing regulations provide a comprehensive framework for legal protection and enforcement.

On the other hand, the organizer of online loans, as the mandatory data controller, must obtain explicit and legitimate consent from data subjects before processing personal data, in accordance with Article 20, paragraph (2), letter a of the PDP Law. If violated, this can result in administrative sanctions. In addition to criminal and administrative sanctions, victims also have the right to submit civil lawsuits to claim compensation for damages, as stipulated in Article 12, paragraph (1) of the PDP Law and Article 26, paragraph (2) of the ITE Law. Thus, even though online loans present risks of non-physical crimes, regulations have provided protection and comprehensive law enforcement mechanisms.

The phenomenon of identity abuse for online loan applications is not merely an individual issue but has escalated into a national legal problem. According to reports from the Financial Services Authority (OJK), throughout 2023, there were over 1.3 million complaints related to online loans, a significant portion of which involved unauthorized use of personal data. Simultaneously, the Illegal Online Loan Eradication Task Force noted that more than 4,000 illegal lending platforms were still operating as of 2024, with the common modus operandi involving data theft and identity misuse for credit applications. This data indicates a systematic and repetitive escalation of cases, highlighting a high level of public vulnerability to this form of crime.

The urgency of studying law enforcement against identity abuse is further underscored by its profound social impacts. Victims are not only burdened by financial

liabilities from loans they never applied for but also face intimidation, defamation, and psychological pressure due to aggressive debt collection practices. Moreover, legal uncertainty becomes palpable when service providers and law enforcement agencies struggle to identify perpetrators, collect viable digital evidence, and evaluate the validity of electronic documents. This situation demonstrates that digital crime threatens not only economic aspects but also erodes public trust in the legal fintech system and financial services.

On the other hand, available academic studies show that, although research on fintech, digital consumer protection, and online loan regulations have been extensively conducted, studies specifically focusing on law enforcement against identity abuse in online loan criminal actions remain very limited (Handoyo, 2023; Juniardana & Kasih, 2022; Kornelis, 2022; Rahman et al., 2023; Silalahi, 2022). Most studies focus on aspects of personal data protection, general fintech regulations, or juridical analysis of illegal loan sharks. However, there has yet to be research that comprehensively connects criminal law instruments, digital evidence mechanisms, and legal certainty concepts in the context of identity abuse. This represents an explicit research gap that calls for a deeper and more structured study.

This research gap is particularly relevant given that the positive legal framework in Indonesia does not yet provide explicit regulations specifically governing identity abuse in online lending transactions. Law enforcement agencies must rely on articles concerning forgery in the Criminal Code (KUHP), provisions in the ITE Law, and the PDP Law, each with different scopes and interpretations. Consequently, law enforcement often lacks consistency, depending heavily on the interpretation of articles by investigators or prosecutors, leading to legal uncertainty for both victims and fintech operators.

The contribution of this study is located in two areas at once. Theoretically, this research enriches the literature on cybercriminal law, particularly related to digital identity and evidentiary mechanisms. Practically, this research provides concrete recommendations for policymakers, OJK, and law enforcement authorities to strengthen legal instruments and improve the effectiveness of handling identity abuse cases in the online loan sector.

This study aims to contribute in two key dimensions. Theoretically, it enriches the literature on cybercriminal law, particularly concerning digital identity and evidentiary mechanisms. Practically, it provides concrete recommendations for policymakers, the OJK, and law enforcement authorities to strengthen legal instruments and improve the effectiveness of handling identity abuse cases in the online lending sector.

Method

This study used a juridical-normative approach (Diantha, 2017; Soekanto & Mamudji, 2011; Soerjono & Soekanto, 2014) designed to produce a comprehensive analysis of law enforcement regarding identity abuse in online loan criminal cases. The methodology suited the normative nature of the problem, which was based on regulations

and required legal interpretation to address emerging digital practices. The research focused on exploring the structure of rules, legal principles, and doctrines forming the framework for law enforcement in Indonesia.

Operationally, the study combined three main approaches common in legal research: the statutory approach, the conceptual approach, and the case approach (Mezak, 2006; Sugiyono, 2015; Suhaimi, 2018). The statutory approach examined relevant legal norms, including the Criminal Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and Financial Services Authority regulations governing online loan services. This aimed to identify the positive legal framework for enforcement against identity abuse perpetrators.

The conceptual approach studied key concepts such as identity theft, cybercrime, digital authentication, and legal certainty in classical and contemporary legal theories. This approach framed identity abuse within a broader theoretical context consistent with international discourse on personal data security and cyber law. It also supported analysis of legal theories from Hans Kelsen, Gustav Radbruch, and modern data protection approaches applied globally.

The case approach analyzed relevant court decisions on identity abuse related to online loans and similar cybercrimes. This identified patterns of accountability, digital evidence methods, and legal norm consistency in practice. Three to five court decisions were purposively selected based on relevance, complexity, and their illustration of challenges in applying positive law.

Legal materials included primary sources—regulations, legislation, and court decisions—the main objects of interpretation. Secondary sources comprised national and international journal articles, cybercriminal law books, official OJK reports, Ministry of Communication and Information publications, and reports from institutions like UNODC and OECD providing comparative perspectives. Tertiary sources such as legal dictionaries and encyclopedias supported definition accuracy and analysis.

Data analysis was qualitative, interpreting legal norms through grammatical, systematic, and teleological techniques. Findings were synthesized with relevant theories and previous studies, linking norms, practices, and social context. This doctrinal approach aligned with international legal research standards, combining theoretical frameworks and empirical case evidence.

The study's stages were designed to be replicable by researchers with access to the same legal materials and interpretative methods, ensuring scientific transparency and accountability in cyber law and fintech research.

Results and Discussion

Framework Regulation and Scope Arrangement Abuse Digital Identity

Research results show that the regulatory framework related to identity abuse in online loan services in Indonesia is still fragmentary in nature (Nurani et al., 2023; Nurfadilah et al., 2023). Although there are several partial regulations that can be used to prosecute perpetrators—such as forgery provisions in the Criminal Code, Articles 26, 30,

and 35 of the ITE Law, and Articles 65–67 of the Personal Data Protection Law (PDP Law)—there are no specific norms that explicitly regulate identity abuse in fintech transactions. This fragmentation causes law enforcement officers to connect various legal instruments that were actually designed for different contexts, which in turn creates a wide room for interpretation in practice.

This condition becomes more complex considering that the operational model of online loans depends heavily on personal data use and digital identity verification. On one hand, personal data protection regulations provide a normative basis regarding the prohibition of data usage without consent. However, on the other hand, the absence of mandatory digital verification standards for fintech organizers makes consistency in law enforcement difficult to achieve. Thus, the existing regulatory framework is not yet fully capable of responding to the development of crime modes that increasingly exploit digital identity and adapt to new technologies.

Findings Empirical Based on Analysis Decision and Report Law enforcement

Analysis of court decisions and official law enforcement reports shows a pattern that identity abuse crimes in online loans almost always involve the manipulation of personal data, either in the form of theft, hacking, or the use of third-party proprietary data obtained through illegal applications (Handoyo, 2023; Muttaqin & Nuryanti, 2023; Salasa Anastasia, 2023; Silalahi, 2022). In some major cases, perpetrators exploit security gaps, such as weaknesses in the online loan authentication system, so that the verification process can be passed with just an uploaded photo of an ID card (KTP) and selfies, which are often easy to falsify.

An important finding is the weakness in the quality of digital evidence submitted to trials. Many cases show that the digital footprint of the perpetrator was not processed in a forensic manner—e.g., document metadata was incomplete, activity logs were not reconstructed properly, or there was no documented chain of evidence (chain of custody) according to international digital forensics standards, such as ISO/IEC 27037. As a result, the evidence often relies on witness descriptions or logical assumptions by investigators, rather than on electronically verified proof in a scientific manner.

These empirical facts confirm that the success of law enforcement depends not only on regulations but also on the capacity of law enforcement institutions to utilize technology and comprehensive digital investigation methods.

Challenge Law Enforcement: Digital Evidence, Cross-Agency Authority, and Anonymity Perpetrator

One of the most significant issues found in this study is the complexity of digital proof. Unlike conventional evidence, digital evidence is intangible, easily modified, and highly dependent on the system where it is stored. A challenge arises when the online lending platform does not provide a detailed log mechanism or when the data is stored with a service provider abroad, who is not subject to Indonesian jurisdiction. This causes

the investigation process to often be hampered at the stage of data requests or the verification of digital devices used by perpetrators.

In addition, coordination between institutions—such as the Police, OJK, Kominfo, and fintech organizers—is still not in line with the principle of integrated law enforcement. There is no integrated database that allows for fast verification of digital identity, activity records, or loan application histories. The fragmentation of authority makes law enforcement slow and inconsistent, especially in cases involving illegal platforms or perpetrators abroad.

From a technical perspective, the anonymity of perpetrators who use VPNs, virtual devices, or unregistered mobile numbers creates additional obstacles for investigators. This condition strengthens Grabosky's theory that cybercrime grows in an ecosystem that provides anonymity, speed, and flexibility in modus operandi, causing law enforcement to always be one step behind the perpetrators.

Relatedness between Law Enforcement and Legal Certainty: Perspective Theoretical and Practical

The findings of this study are in harmony with Gustav Radbruch's theory of legal certainty, which states that legal norms cannot function optimally without consistent enforcement and predictable laws (Chandra Saputra, Ma'rifah, 2021; Intan Audya, Jeanne DN Manikb, 2021). In the context of digital identity abuse, unclear norms and inconsistencies in enforcement cause uncertainty for the community, fintech organizers, and law enforcement agencies.

In practice, legal uncertainty is reflected in the variation of articles used to ensnare perpetrators, differences in digital proof procedures between legal areas, and the absence of standard operating procedures in digital identity crime investigations. This uncertainty has implications for the decline in public trust in the protection of state law, especially for victims who are trapped in loans they did not apply for.

From a theoretical perspective, these findings indicate the need to update laws that not only focus on tightening sanctions but also on strengthening digital forensics infrastructure, unifying investigation procedures based on technology, as well as harmonizing fintech regulations and personal data protection. Effective law enforcement must be viewed as a combination of clear norms, adequate institutional capacity, and the utilization of technology in line with the dynamics of digital crime.

Implications Findings for Strengthening Regulations and Practices Law enforcement

As part of the discussion, it is important to emphasize that the results of this study lead to the need for strengthening regulations in a structural way. Indonesia needs to consider the formation of special regulations related to digital identity abuse, similar to the Identity Theft Enforcement and Restitution Act in the United States or the General Data Protection Regulation (GDPR) in the European Union, which regulates in detail the

use of personal data and accountability for its misuse (Doyle, 2013; Li et al., 2019; UK Information Commissioner's Office, 2019; Zhang et al., 2020).

In addition, the implementation of identity verification standards based on biometrics and liveness detection technology is required for all online loan organizers, both legal and illegal, that will be eradicated. Strengthening the capacity of agencies in the field of digital forensics, especially in the identification process of devices, metadata analysis, and the reconstruction of digital footprints, is a prerequisite for effective and consistent law enforcement.

At the public policy level, data integration between institutions needs to be realized in the form of the National Digital Identity Verification System, which allows for fast validation of loan applicants' identities. This step will not only increase the efficiency of law enforcement but also provide legal certainty for the public by ensuring that digital systems can verify identities accurately before loans are approved.

Conclusion

This study demonstrates that identity abuse in online loan crimes is a rapidly evolving form of cybercrime driven by digital transformation in financial services. Perpetrators exploit weaknesses in digital verification systems and legal frameworks that have not kept pace, resulting in inconsistent and often ineffective law enforcement. Key challenges include inadequate digital evidence, limited forensic capabilities, and poor coordination among institutions. To address these issues, urgent legal reforms are needed, such as creating specific regulations on digital identity abuse, enhancing forensic capacity, adopting biometric verification technologies, and enabling cross-border data integration. These measures aim to strengthen legal certainty, improve enforcement effectiveness, and restore public trust. Future research should explore the development and impact of interoperable digital identity systems and the role of emerging technologies in preventing identity abuse.

References

Arkaan Daffa, & Sidi Ahyar Wiraguna. (2025). Pelanggaran Privasi Nasabah : Analisis Hukum Atas Praktik Pembocoran Data Oleh Bank Kepada Mata Elang. *Jembatan Hukum : Kajian Ilmu Hukum, Sosial Dan Administrasi Negara*, *2*(2), 293–304. Https://Doi.Org/10.62383/Jembatan.V2i2.1737

Chandra Saputra, Ma'rifah, Masdari. T. (2021). Abstract Implications Of Transfer Of Authority Of Legal Assurance Oriented. *De Jure Critical Laws Journal*, *2*(2).

Diantha, I. M. P. (2017). Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum. In *Hukum Normatif Dalam Justifikasi Teori Hukum*.

Ekayani, L., Djanggih, H., & Suong, M. A. A. (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan. *Journal Of Lex Philosophy (JLP)*, *4*(1). Https://Doi.Org/10.52103/Jlp.V4i1.1485

Handoyo, E. R. (2023). Urgence Of Data Protection Regulation Updates For Consumers As Users Of Online Loan Applications. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *9*(2). Https://Doi.Org/10.33330/Jurteksi.V9i2.2150

Intan Audya, Jeanne D.N Manikb, W. (2021). Kajian Hukum Asas Retroaktif Dalam Kejahatan Terhadap Kemanusiaan. *Jurnal Hukum*, *7*(1).

Juniardana, I. G. A., & Kasih, D. P. D. (2022). Urgensi Regulasi Financial Technology (Fintech) Pinjaman Online Melalui Pembayaran Perbankan. *Kertha Semaya : Journal Ilmu Hukum*, *10*(10). Https://Doi.Org/10.24843/Ks.2022.V10.I10.P09

Kornelis, Y. (2022). DIGITAL BANKING CONSUMER PROTECTION: DEVELOPMENTS & CHALLENGES. *Jurnal Komunikasi Hukum (JKH)*, *8*(1). Https://Doi.Org/10.23887/Jkh.V8i1.44477

Muttaqin, I., & Nuryanti, L. (2023). Online Loan Phenomenon Among Students: Micro And Macro Psychological Analysis Fenomena Pinjaman Online Di Kalangan Mahasiswa: Analisis Psikologi Mikro Dan Makro. *Jurnal Pemikiran Dan Penelitian Psikologi*, *18*(2).

Nurani, E., Wiryanto, W., & Riyanto, S. (2023). Optimalisasi Perlindungan Konsumen Atas Kebocoran Pengelolaan Data Pribadi Dalam Pinjaman Online. *Jurnal Hukum Jurisdictie*, *5*(2). Https://Doi.Org/10.34005/Jhj.V5i2.133

Nurfadilah, N., Diab, A. L., & Djaoe, A. N. M. (2023). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online. *FAWAID: Sharia Economic Law Review*, *4*(2). Https://Doi.Org/10.31332/Flr.V4i2.4424

Pakpahan, B. J. (2021). Mencari Definisi Kehadiran Antar-Subjek Yang Bermakna Di Ruang Digital. *BIA': Jurnal Teologi Dan Pendidikan Kristen Kontekstual*, *4*(1). Https://Doi.Org/10.34307/B.V4i1.219

Rahman, I., Sahrul, Mayasari, R. E., Nurapriyanti, T., & Yuliana. (2023). Hukum Perlindungan Konsumen Di Era E-Commerce: Menavigasi Tantangan Perlindungan Konsumen Dalam Lingkungan Perdagangan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *2*(08). Https://Doi.Org/10.58812/Jhhws.V2i08.605

Risdiany, H., Sukmalia, M., & Suargana, L. (2024). Pemahaman Mendalam: Dampak Smartphone Pada Eksistensi Manusia Dalam Filsafat Teknologi. *UPGRADE : Jurnal Pendidikan Teknologi Informasi*, *1*(2). Https://Doi.Org/10.30812/Upgrade.V1i2.3557

Salasa Anastasia, D. (2023). Urgensi Pembentukan Hukum Fintech Untuk Memberi Perlindungan Hukum Kepada Konsumen Dalam Pinjaman Online. *Jurnal Hukum Dan HAM Wara Sains*, *2*(02). Https://Doi.Org/10.58812/Jhhws.V2i02.227

Silalahi, W. (2022). Urgensi Perlindungan Konsumen Berbasis Teknologi Digital (The Urgence Of Consumer Protection Based On Digital Technology). *Prosiding Seri Seminar Nasional*, *2*(1).

Siti Maesaroh, R. (2025). Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(2), 255–274. Https://Doi.Org/10.14421/3n8bxw79

Sugiyono. (2015). Metode Penelitian Dan Pengembangan Pendekatan Kualitatif, Kuantitatif, Dan R&D. In *Metode Penelitian Dan Pengembangan Pendekatan Kualitatif, Kuantitatif, Dan R&D*.

Suhaimi. (2018). Problem Hukum Dan Pendekatan Dalam Penelitian Hukum Normatif. *Jurnal Yustitia*, *19*(2).

Trisilowati, D. (2017). EKSISTENSI DAN IDENTITAS DI MEDIA BARU. *Jurnal Komunikasi*, *11*(1). Https://Doi.Org/10.21107/Ilkom.V11i1.2837

UK Information Commissioner's Office. (2019). Guide To The General Data Protection Regulation (GDPR). *Guide To The General Data Protection Regulation*, *May*.

Wibowo, A., Kom, M., & Si, M. (2023). Hukum Di Era Globalisasi Digital. *Penerbit Yayasan Prima Agus Teknik*.

Zen Munawar, Iswanto, Dandun Widhiantoro, Novianti Indah Putri, & Komalasari, R. (2022). Keamanan, Data Pribadi Pada Metaverse. *TEMATIK*, *9*(2). Https://Doi.Org/10.38204/Tematik.V9i2.1069

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online Customer Trust In The Context Of The General Data Protection Regulation (GDPR). *Pacific Asia Journal Of The Association For Information Systems*, *12*(1). Https://Doi.Org/10.17705/1pais.12104