

## **CRIMINAL LIABILITY OF ONLINE FRAUD PERPETRATORS THROUGH ILLEGAL ONLINE LOAN APPLICATIONS**

**Reny Okprianti<sup>1\*</sup>, Nur Husni Emilson<sup>2</sup>, Muhammad Rafli<sup>3</sup>, Amanda Prattiwy<sup>4</sup>, Wanda Puja Octavia<sup>5</sup>, Frity Vania Zerlinda<sup>6</sup>**

<sup>1,2,3,4,5,6</sup>Faculty of Law, Muhammadiyah University of Palembang, Palembang, Indonesia  
renyveltini@gmail.com<sup>1\*</sup>, nur.husni@gmail.com<sup>2</sup>, m.rafli@gmail.com<sup>3</sup>,  
amanda@gmail.com<sup>4</sup>, wanda@gmail.com<sup>5</sup>, frity@gmail.com<sup>6</sup>

### Abstract

The rapid development of technology has had an impact on changes in people's lifestyles, where things can be done quickly and easily using online-based services or using the internet network, whether in terms of shopping transactions, booking hotels, paying electricity bills, train tickets, plane tickets, or making money or capital loan transactions online. The method used is normative legal research with a library research approach, which examines literature, laws and regulations, and relevant legal documents. The results of the study show two main findings. First, illegal online loan providers can be held accountable civilly, criminally, and administratively. In the civil realm, they are required to compensate for losses based on Article 1365 of the Civil Code. In the criminal realm, perpetrators can be charged with articles related to extortion, misuse of personal data, and fraud. Meanwhile, administratively, the OJK has the authority to impose sanctions such as license revocation and access blocking based on POJK No. 77/POJK.01/2016. Second, delinquent debtors who utilize illegal online loans to commit fraud, such as identity falsification or fictitious loans, can be charged with Article 378 of the Criminal Code if there is evidence of malicious intent. The implications of this research are the need to increase public awareness of the right to personal data privacy, strengthen law enforcement, and update policies in accordance with the dynamics of the digital era.

Keywords: Technology, Online Fraud, Illegal Online Loans

## **INTRODUCTION**

Advances in digital technology have made financial services increasingly accessible. One popular service is online lending (pinjol). However, this convenience has also given rise to abuse by irresponsible parties through illegal lending apps. Illegal lending typically offers fast processing without verification, but traps victims with high interest rates, personal data theft, and other forms of fraud. According to 2023 OJK data, more than 4,000 illegal lending sites and apps have been blocked, indicating that this crime is growing rapidly and is organized. The losses to society are not only material, but also psychological and social (Ningsih & Rochmani, 2025).

This phenomenon not only causes material losses but also has psychological impacts, as victims often receive threats or intimidation. Therefore, it is crucial to understand how the Indonesian legal system assigns criminal liability to perpetrators and how regulations protect the public from digital financial crime. Although regulations related to fintech lending are in place, numerous legal loopholes remain, exploited by perpetrators. Perpetrators generally operate in an organized manner, using servers located overseas, and exploiting the public's low digital literacy. This situation demonstrates that law enforcement requires a more comprehensive approach, encompassing not only regulations but also inter-agency coordination and public education. Therefore, discussing the criminal liability of perpetrators of online fraud through illegal online lending applications is crucial for analyzing how criminal law operates in the face of increasingly complex digital crimes (Kurniawan et al., 2023).

## **RESEARCH METHODS**

This study uses a normative legal research method, namely research that focuses on the study of written legal norms and relevant legal materials. The normative approach was chosen because the issue of criminal liability in cases of online fraud through illegal online loan applications is essentially an issue that can be analyzed through applicable legal instruments in Indonesia. This method emphasizes the exploration and analysis of various laws and regulations such as the Criminal Code, the ITE Law, the Consumer Protection Law, and the Financial Services Authority (OJK) Regulations related to fintech lending, supplemented by a review of academic literature from relevant scientific journals. The analysis was conducted to understand how positive law regulates, ensnares, and provides the basis for criminal liability for perpetrators of online fraud through illegal online loans.

## **RESULT AND DISCUSSION**

### **A. Characteristics and Modus Operandi of Illegal Loan Fraud**

Online fraud perpetrated through illegal lending apps is a result of advances in financial technology that are not fully aligned with regulations and the public's digital literacy. Although the government has enacted laws to monitor and prosecute violations in the fintech sector, illegal lenders exploit legal loopholes, lack of public understanding, and the ease of technology to perpetrate organized crime. Illegal lenders typically lack permits from the Financial Services Authority (OJK). Their apps can be downloaded through social media, unofficial links, or APK files. Some of the most common methods are as follows (Kusuma et al., 2023):

1. Misuse and Theft of Personal Data

Unauthorized apps request full access to the user's contacts, photo gallery, location, and other data stored on their phone. As Shonhadji explained, the perpetrators use this data to inflict psychological pressure on the victim, then use it to threaten and humiliate them.

## 2. Sending Funds Without Approval

Victims suddenly receive money from illegal apps and are then forced to repay it with compounded interest. Imanuddin's report found this method to be a trap designed to create a false legal relationship between the perpetrator and the victim (Manik et al., 2023).

## 3. Unreasonable Interest and Unlawful Collection Practices

Interest rates can rise to forty to one hundred percent in a matter of days. Collection is carried out through WhatsApp spam, intimidation, doxing, and the spread of slander to the victim's contacts.

## 4. Hidden Company Identity And Server

Located overseas (Singapore, India, Cambodia), making them difficult for authorities to track. Manik pointed out that many illegal online loan operators have international networks. Fraud through illegal online loans exhibits characteristics of organized crime because perpetrators operate not only as individuals but often form networks with operational structures, IT systems, and collection divisions, and money laundering techniques. Ralang Hartati & Syafrida showed that the perpetrator group used various digital platforms such as Telegram, WhatsApp Business, and temporary website domains to quickly move servers when detected by the government. Furthermore, several studies in 2023–2024 found the use of facial recognition algorithms in the fake verification process. This demonstrates how modern technology is used to convince victims that the service is "similar to a legitimate application." These results reinforce the idea that illegal online lending exploits psychological weaknesses, technological limitations, and inability to detect society.

## **B. Basis for Criminal Responsibility of Illegal Loan Perpetrators**

The Indonesian legal system is comprehensive enough to prosecute online fraudsters. Recent legal developments have made illegal online lenders criminally liable. This amendment refers not only to the Criminal Code (KUHP) and the ITE Law, but also to the Personal Data Protection Law, which clarifies the categories of violations related to the collection, processing, and dissemination of personal data without consent. This aligns with Hanifawati's (2022) analysis, which states that privacy violations are the primary mode of crime committed by illegal online lenders. Therefore, the implementation of the Personal Data Protection Law could increase enforcement. Furthermore, to involve other parties, such as server providers, application script providers, or billing operators, Articles 55 and 56 of the Criminal Code concerning complicity (*deelneming*) can be used. This method makes sense because the majority of illegal online lenders work together (Lubis, 2025).

1. Articles 378 and 368 of the Criminal Code concerning fraud and extortion, as well as Article 368 of the Criminal Code concerning extortion (intimidation during debt collection), provide an opportunity for perpetrators of crimes who violate the law to be subject to cumulative penalties.
2. ITE Law No. 11 of 2008 in conjunction with Law No. 19/2016 covers illegal access to electronic systems, unauthorized data transmission, manipulation and theft of personal data, and sending threats and terror through electronic media. Hanifawati emphasized that misuse of personal data is the basis of illegal online loan crimes.
3. According to the Consumer Protection Law (UUPK), perpetrators can be considered to have committed the following: fraudulent practices, dissemination of incorrect information, and billing that is detrimental to consumers.
4. POJK 77/2016, which relates to Fintech Lending, stipulates that:
  - a. Organizers must be registered or licensed;
  - b. Data security must be maintained; and

- c. Collections that contain violence or threats are prohibited.

The perpetrator who breaks the law violates all of these points, so the act can be considered a criminal offense.

### C. Form of Legal Responsibility of Violators

From a legal perspective, this encompasses aspects of legal fault, legal causation, and the capacity to bear legal responsibility. Corporate liability in this crime becomes increasingly relevant because most applications are managed under the name of foreign legal entities. According to Lubis' analysis, the operational model in question allows violators to shift responsibility to dummy companies. Therefore, the application of the doctrine of vicarious liability and corporate mens rea is highly relevant for prosecuting the capital of owners, system operators, and those who provide operational instructions (Kurniyanto et al., 2025).

Regarding intent (*dolus*), the intent in this case is *dolus directus*, as the perpetrator clearly directed his actions to defraud and obtain illegal gain. However, it is also possible that it involves *dolus eventualis*, where the perpetrator was aware of the risk of disclosing the victim's personal data but proceeded anyway for financial gain.

#### 1. Intention (Mode)

The offender knowingly:

- a. create mobile applications to cheat,
- b. using threats,
- c. profit from unreasonably high interest rates.

Illegal online loan fraud is not an act of negligence but premeditated behavior.

#### 2. Corporate Responsibility

Violators often take the form of fictitious 'companies'.

According to Ningsih & Rochmani's study, companies can also be punished if:

- a. mistakes made by the leadership;
- b. proceeds of crime enter the business entity; or
- c. operational systems used for fraud

#### 3. Layered accountability

Fraud, Article 378 of the Criminal Code, extortion, Article 368 of the Criminal Code, data misuse, Article 32 of the ITE Law, and digital terror, Article 29 of the ITE Law. Lubis's (2025) findings indicate that a multi-article approach is needed to address illegal online loans.

#### 4. Law Enforcement Obstacles

Despite the adequate basis, law enforcement still faces many challenges. Digital evidence also hinders law enforcement. Many apps use layered encryption, VPNs, and international cloud servers, making seizures difficult.

#### 5. Electronic Evidence

Kurniawan stated that the primary evidence of illegal online lending lies in metadata, server history, DNS records, and digital transactions, which are difficult to access without international cooperation. Therefore, authorities require more advanced digital forensics skills. Furthermore, victims have not fully utilized public reporting tools such as the Kominfo Content Complaint Application and the OJK consumer service because many are unaware of the complaint procedures or feel the process is too long (Imanuddin et al., 2022).

6. Seizing digital devices and servers is extremely difficult because the perpetrators and servers are located abroad. This lengthy process requires international cooperation from authorities.

7. Lack of digital literacy: Many victims don't know how to verify whether an app is

legitimate. Kurniyanto et al. stated that most users download apps through unofficial links.

8. Reasons why victims are reluctant to report include: fear of intimidation, embarrassment, or not knowing legal procedures.
9. Limitations in coordination between the OJK, Kominfo, and Polri, who must work together, are often hampered by bureaucracy, as noted by Manik et al. (2023).

Real Case Example:

- 1) The "Tsunami of Online Loans" case in Yogyakarta in 2022 revealed that students fell victim to illegal online loans after receiving 36 applications. The perpetrators spread threats with the victim's personal photos, disseminated information to contacts, and charged interest rates exceeding 60% weekly. Police followed up with multiple charges, including the Electronic Information and Transactions Law (UU ITE) and the Indonesian Criminal Code (KUHP).
- 2) In cases of unconsented money transfers, the victims did not request a loan, but received an automatic transfer. The perpetrators were accused of digital violence. Imanuddin et al.'s findings suggest a similar modus operandi. Another example is the case in Jakarta and Yogyakarta. Hidayah's study showed that students experienced significant psychological distress due to involvement in forty illegal online loan applications. This phenomenon suggests that perpetrators exploit not only lower-middle-class communities but also educated groups, who remain vulnerable when perpetrators use financial and emotional pressure.
- 3) Another case in 2024 revealed that an illegal loan shark network based in Cambodia targeted Indonesians through hundreds of web domains and billing services through a shady call center. This case demonstrated the perpetrators' technical capabilities and international networks, necessitating multi-country cooperation to resolve the issue.

#### **D. The Need for Broader Regulatory Updates**

Regulatory reforms are needed to address legal inconsistencies regarding international jurisdiction, data security, and application oversight on digital platforms. Manik et al. (2023) emphasize that to prevent overlapping authority, the Financial Services Authority (OJK), the Ministry of Communication and Information Technology (Kominfo), Bank Indonesia (BI), and law enforcement agencies must collaborate on regulations. Furthermore, regulatory reforms are needed to improve mechanisms for direct disclosure of legal violations and to expand cross-border investigative cooperation through mutual legal assistance (MLA). Because most fraud victims are caused by ignorance and economic pressures, not technology, However, this effort must be accompanied by increasing digital and financial literacy in society.

The existence of the ITE Law and the POJK is not sufficient to combat transnational crime. What is needed is:

1. Cross-Jurisdictional Fintech Regulatory Update,
2. Stronger Personal Data Protection Regulations,
3. Digital Forensics-Based Law Enforcement,
4. International Cooperation on Cybercrime.

The Social and Psychological Impact of Illegal Online Loan Fraud Victims not only suffer financial losses due to fraud through illegal online loan applications but also experience significant social and psychological impacts. Threats, intimidation, and the dissemination of personal data cause psychological distress for many victims. According to Hidayah, digital threats can cause mental distress, sleep disturbances, depression, long-term anxiety, and fear of meeting other people. Victims may even face social isolation due to shame and stigma

(Hartati & Syafrida, 2022). Many illegal applications are distributed through Facebook, TikTok, and WhatsApp, so platforms must improve ad verification and public reporting features to remove illegal online loan promotional accounts more quickly (Shonhadji, 2022).

## CONCLUSIONS

The phenomenon of fraud through illegal loan apps demonstrates that technological advancements are not only profitable but also open up opportunities for new and increasingly complex crimes. The modus operandi used by perpetrators, which includes data theft, unilateral disbursement of funds, unreasonable interest rates, and threats and harassment, demonstrates that illegal lending is a form of organized cybercrime. In the case of fintech lending, the Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), the Consumer Protection Law, and the POJK (OJK Regulation) have established a clear basis for criminal liability in the Indonesian legal system. Fraud, extortion, illegal access, and misuse of personal data are some examples of offenses that can ensnare perpetrators.

## REFERENCES

- Hartati, R., & Syafrida. (2022). Legal protection for consumers of illegal online loans (illegal online loans). *Otentik's: Jurnal Hukum Kenotariatan*, 4(2). <https://doi.org/10.35814/otentik.v4i2.3737>
- Imanuddin, I., Anggraeni, R. R., Fridayani, F., & Susanto, S. (2022). Construction of consumer protection against illegal online loan transactions as a means of ius constituendum in Indonesia. *IUS: Kajian Hukum dan Keadilan*, 11(3). <https://doi.org/10.29303/ius.v11i3.1312>
- Kurniawan, I. D., Ismunarno, & Suyatno. (2023). Legal protection for online loan customers. *Jurnal Kewarganegaraan*, 7(1). <https://doi.org/10.31316/jk.v7i1.5154>
- Kurniyanto, D., Dewi, P. M., & Putri, F. A. J. (2025). Legal protection for consumer risks from illegal online lending practices. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 3(3), 2448–2455. <https://doi.org/10.62976/ijijel.v3i3.1291>
- Kusuma, A. A. G. C., Mahendrawati, N. L. M., & Arini, D. G. D. (2023). Perlindungan hukum bagi konsumen dalam praktik bisnis pinjaman online ilegal. *Jurnal Konstruksi Hukum*, 3(2), 426–431. <https://doi.org/10.22225/jkh.3.2.4850.426-431>
- Lubis, Y. P. (2025). Penyelidikan hukum pidana dalam penanganan kasus pinjaman online ilegal. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(3). <https://doi.org/10.61104/alz.v3i3.1606>
- Manik, P. S., Simanungkalit, J., Simanjuntak, F. F., Saragih, A. L., & Hasyim, H. (2023). Legalitas bisnis pinjaman online: Studi kasus terhadap praktik fintech ilegal di Indonesia. *Jurnal Pendidikan Tambusai*, 9(2). <https://doi.org/10.31004/jptam.v9i2.28261>
- Ningsih, I. N., & Rochmani. (2025). Criminal accountability for illegal online loans that conduct crime in the form of peer-to-peer lending in the community. *Awang Long Law Review*, 5(2). <https://doi.org/10.56301/awl.v5i2.684>
- Shonhadji, N. (2022). Fraud analysis on illegal online lending using Habermas' theory of the public sphere. *Jurnal Ilmiah Akuntansi dan Bisnis*, 17(1). <https://doi.org/10.24843/JIAB.2022.v17.i01.p03>