E-ISSN : 2963-4946
Vol. 4 No. 8 May 2026
https://ajosh.org/

Asian Journal of Social and Humanities

# Legal Updates on Handling Identity Theft Crimes in Cross-Border E-Commerce Transactions

**Edy Krispono* , Dwi Kusumo Wardhani**
Universitas Borobudur, Indonesia
Email: edykrispono2104@gmail.com* , dwi_kusumo@borobudur.ac.id

**Keywords:**
identity theft; cross-border e-commerce; cybercrime

**ABSTRACT**

This study aims to analyze and formulate legal reforms in handling identity theft crimes in cross-border e-commerce transactions using normative juridical methods through legislative and conceptual approaches. The results of the study indicate that the legal provisions contained in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 27 of 2022 concerning Personal Data Protection, do not explicitly regulate identity theft as a separate crime and remain fragmentary, thus unable to encompass the complexity of crimes in cross-border digital transactions. Furthermore, normative and implementative weaknesses were found, including the absence of a legal definition of identity theft, weak victim protection, limited recovery mechanisms, and obstacles to cross-border law enforcement, such as jurisdictional conflicts and limited international cooperation. Therefore, legal reform is needed through the establishment of specific norms for identity theft, the strengthening of personal data protection, the regulation of digital platform responsibilities, and the enhancement of international cooperation and law enforcement capacity. This research produces a legal policy model that is preventive, repressive, and restorative in order to ensure the security of cross-border e-commerce transactions and protect Indonesia's data sovereignty.

## INTRODUCTION

The development of digital transformation has significantly driven the growth of the global and national digital economy, particularly through the expansion of cross-border e-commerce, which is increasingly erasing conventional jurisdictional boundaries (Sudiantini et al., 2023). In Indonesia, the digitalization of trade through global marketplaces, electronic payment systems, and fintech integration has made cross-border transactions a common practice in people's economic activities (Manurung, 2024). This condition has created a high dependence on digital identity systems such as user accounts, personal data, and electronic authentication mechanisms as a basis for trust in transactions. However, the globalization of digital transactions has also given rise to new legal risks, particularly related to identity misuse, which is difficult to control given the borderless nature of cyberspace (Kriswandaru, 2026). In this regard, national law faces challenges in keeping pace with the dynamics of rapidly developing technology, so an adaptive legal framework is needed that is capable of guaranteeing security and legal certainty in cross-border e-commerce transactions (Fitriani et al., 2025).From a legal perspective, identity theft is a form of modern cybercrime that involves the unauthorized acquisition and misuse of a person's personal data for specific benefit. Criminologically, this crime has developed through various methods such as account takeover, phishing, social engineering, data breaches, and credential stuffing (Sulaeman & Kemala, 2025). Legally, identity theft is not explicitly regulated in Indonesian positive law but can be

constructed through various scattered provisions. The main elements of identity theft include the acquisition of personal data, the misuse of identity, and the resulting financial and reputational losses to the victim. Unlike conventional fraud, identity theft is data- and technology-based, making it more complex in terms of evidence and law enforcement (Anugerah & Tantimi, 2022). Therefore, identity theft should be positioned as a form of cybercrime that requires a special legal approach and cannot be fully resolved through traditional criminal law instruments.The anonymous and borderless nature of cross-border e-commerce transactions, and the involvement of multiple legal jurisdictions, further increase the vulnerability to identity theft. The use of global platforms and international payment gateways complicates the determination of applicable law, while authentication systems such as passwords, OTPs, and biometrics still have security gaps that can be exploited (Rahayu & Padli, 2023). Furthermore, digital transaction chains involving multiple parties increase the risk of personal data leakage, which ultimately has the potential to be misused for illegal purposes (Purba & Mauluddin, 2023). From a consumer protection perspective, this situation demonstrates the weak position of consumers in cross-border transactions, due to the lack of effective protection against identity theft. This underscores that national laws are not yet fully capable of addressing the complexities of global digital transactions.The escalation of identity theft cases in e-commerce shows an increasing trend both globally and regionally, including in Indonesia, with crime patterns becoming increasingly organized and utilizing advanced technology (Bego, Aziz, Rahmad, & Budianto, 2025). Modus operandi such as phishing, account hacking, and the misuse of data resulting from system leaks indicate that criminals are increasingly adapting to technological developments. The resulting impact is felt not only by individuals in the form of financial and reputational losses, but also by businesses through decreased consumer trust, and by the state in the form of disruptions to the stability of the digital economy (Nafi'ah, 2020). Empirically, many identity theft cases are not resolved effectively due to the legal system's limitations in identifying and prosecuting perpetrators, who often reside outside national jurisdiction (Salsabila & Ilmih, 2024).Within the Indonesian legal framework, regulations related to identity theft can be found implicitly in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, specifically Article 30 concerning illegal access, Article 32 concerning the alteration and transfer of electronic information, and Article 35, which regulates the manipulation of electronic information. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection, through Articles 65 and 67, prohibits the unlawful acquisition and use of personal data (Alkadrie, 2023). However, these regulations remain partial and do not explicitly address identity theft as a separate offense. Links to existing provisions in the Criminal Code, such as Article 378 on fraud and Article 263 on forgery, also fail to fully accommodate the characteristics of digital data-based crimes, creating uncertainty in legal application (Nurdiani, 2020).These weaknesses in legal regulations are further exacerbated by various challenges in cross-border law enforcement, such as jurisdictional issues, legal conflicts, extradition difficulties, and differences in evidentiary standards between countries. Furthermore, the role of global digital platforms, which is not yet optimally regulated in national law, and the weak responsibility of service providers for user identity protection, indicate a significant gap in norms (Arey, Hehanussa, & Salmon, 2025). From a consumer protection perspective, the absence of a clear compensation mechanism and low digital literacy

further worsen the victims' situation. Therefore, comprehensive legal reform is needed through the establishment of specific norms regarding identity theft, the strengthening of personal data protection, the regulation of cross-border e-commerce, and the enhancement of international cooperation (Engidaw, Yu, & Weikang, 2025; Kamisetty, 2024). This approach must be preventive, repressive, and restorative to ensure digital economic security, increase public trust, and safeguard national data sovereignty amidst the current of technological globalization.The urgency of this research is driven by the increasing number of identity theft cases in cross-border e-commerce, the normative weaknesses in existing laws, and the enforcement challenges posed by transnational cybercrimes. Without immediate legal reform, Indonesia risks losing its data sovereignty, experiencing decreased public trust in digital transactions, and facing prolonged economic instability. The novelty of this research lies in its comprehensive legal policy model that not only proposes amendments to existing cyber laws but also integrates international cooperation mechanisms, platform liability standards, and victim protection schemes. The purpose of this study is to analyze current legal provisions on identity theft and formulate a legal reform model applicable to cross-border e-commerce transactions. The contribution of this research is to provide concrete recommendations for policymakers, law enforcement agencies, and digital platforms. The benefits include enhanced legal certainty, improved victim protection, and strengthened national data sovereignty.

## METHOD

This research is a normative juridical study that focuses on the analysis of positive legal norms in examining the problem of identity theft crimes in cross-border e-commerce transactions, using a legislative approach and a conceptual approach. The legislative approach is carried out by systematically reviewing various relevant regulations, particularly Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection, as well as provisions in the Criminal Code relating to fraud and forgery, in order to identify normative gaps, inconsistencies, and weaknesses in legal regulations pertaining to the handling of identity theft. Meanwhile, the conceptual approach is used to examine relevant legal doctrines and theories, such as the concept of cybercrime, personal data protection, electronic commerce law, and legal responsibility in cross-border digital transactions, in order to build a comprehensive legal argument. The legal materials used consist of primary legal materials in the form of statutory regulations, secondary legal materials in the form of scientific literature, journals, and previous research results, as well as tertiary legal materials as supporting references, which are then analyzed qualitatively through legal interpretation techniques and prescriptive arguments to produce recommendations for legal reforms that are adaptive to technological developments and the complexity of transnational cybercrime.

## RESULT AND DISCUSSION

### Positive Legal Regulations on Identity Theft Crimes in Cross-Border E-Commerce Transactions

Positive legal regulations on identity theft crimes in cross-border e-commerce transactions in Indonesia are still primarily based on a general cyber law regime scattered

across various laws and regulations. Normatively, the main framework for these regulations is contained in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, the most recent amendment to the legal regime for electronic information and transactions in Indonesia. This law regulates various acts related to illegal access, data manipulation, and misuse of electronic systems, but does not explicitly regulate identity theft as a separate crime. Consequently, legal construction regarding identity theft still requires interpretation of scattered norms, which implies a lack of legal certainty in handling it (Mahmud, 2019).

Regarding illegal access as the initial stage of identity theft, Article 30 paragraphs (1), (2), and (3) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions prohibit anyone from gaining unauthorized access to electronic systems for the purpose of obtaining electronic information or electronic documents. This provision is relevant to the practice of identity theft, which generally begins with the hacking of an account or system to obtain the victim's personal data (Widhaningroem, 2024). However, this norm only regulates the aspect of illegal access without explicitly addressing the misuse of the acquired identity, thus not reflecting the entire series of actions involved in identity theft, which are multi-layered and ongoing. Article 32 paragraphs (1), (2), and (3) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions prohibit the unauthorized alteration, addition, reduction, transmission, destruction, removal, transfer, or concealment of electronic information. This provision can be linked to acts of data manipulation in identity theft, such as account takeovers or changes to identity information in electronic systems. Furthermore, Article 35 regulates acts of manipulation, creation, alteration, removal, or destruction of electronic information with the aim of making it appear as though the data is authentic (Mahameru et al., 2023). This norm has significant relevance to identity theft because it reflects elements of identity falsification in the digital space, but it still does not explicitly mention identity theft as a separate crime.

Regulations related to the protection of personal data as the primary object of identity theft are stipulated in Law Number 27 of 2022 concerning Personal Data Protection, specifically Article 65 paragraph (1), which prohibits any person from obtaining or collecting personal data that does not belong to them with the intent to unlawfully benefit themselves or others, and Article 67, which regulates criminal sanctions for such violations. These provisions provide a more specific legal basis for protecting personal data as a primary element in identity theft. However, this law's primary focus is on protecting data subjects, not on the overall crime of identity theft. Consequently, there are still limitations in addressing the dimensions of identity misuse in cross-border e-commerce transactions (Gabriel, 2024).

Beyond the cyber law regime and personal data protection, identity theft can also be linked to provisions in the Criminal Code, specifically Article 263 concerning document forgery and Article 378 concerning fraud. Article 263 can be used to prosecute the act of falsifying identity in the form of electronic documents, while Article 378 relates to the use of a false identity to obtain unlawful gain. However, the application of these provisions to digital-based crimes faces challenges due to the intangible nature of the objects and the complexity of the technology used (Adelika, 2023). This demonstrates that conventional criminal law has not fully adapted to developments in cybercrime, such as identity theft.

It can be concluded that positive legal regulations in Indonesia have a normative basis for prosecuting identity theft perpetrators through various provisions spread across Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and the Criminal Code. However, these regulations remain fragmentary, unsystematic, and do not explicitly regulate identity theft as a separate crime, thus failing to address the complexity of this crime in the context of cross-border e-commerce transactions. This concern underscores the need for more comprehensive and integrated legal reforms to provide legal certainty and effectiveness in combating identity theft in the digital era.

**Weaknesses and Challenges in Law Enforcement Against Identity Theft in Cross-Border E-Commerce**

One normative weakness in handling identity theft in Indonesia lies in the lack of an explicit legal definition of identity theft in legislation. In Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, although there are provisions regarding illegal access in Article 30 and manipulation and alteration of data in Articles 32 and 35, there is no single provision that expressly qualifies identity theft as a separate offense. Empirically, this situation forces law enforcement officials to construct articles cumulatively, which often does not reflect the entire chain of actions of the perpetrator, potentially leading to legal uncertainty and disparity in decisions in judicial practice.

Furthermore, legal norms governing identity theft are scattered and unsystematic, both within the cyber law regime and personal data protection. Law Number 27 of 2022 concerning Personal Data Protection, specifically Article 65 paragraph (1) and Article 67, does indeed regulate the prohibition on obtaining and using personal data unlawfully, but this provision focuses more on protecting data as an object, rather than on misuse of identity as a complete crime. Empirically, this results in many identity theft cases not being handled optimally due to the lack of a clear legal framework regarding the relationship between data collection, identity misuse, and victim losses within a comprehensive criminal framework.

Another weakness lies in the inadequate protection of victims and remedies. Although Law Number 27 of 2022 concerning Personal Data Protection grants data subjects the right to obtain protection for their personal data, regulations regarding compensation or restitution for losses resulting from identity theft remain unclear and have not been effectively implemented. Empirically, identity theft victims often suffer financial and reputational losses without a swift and effective remedy mechanism, and face difficulties in holding accountable parties negligent in protecting personal data, including digital platforms.

In cross-border e-commerce, law enforcement challenges are further complicated by differences in jurisdiction and conflicts of law between countries. The borderless nature of transactions makes it difficult to determine which law applies (choice of law) and which jurisdiction has jurisdiction to prosecute. Empirically, many identity theft cases involve perpetrators located outside of Indonesia, making law enforcement processes such as investigation, arrest, and extradition extremely difficult. Limited international cooperation and differences in legal systems between countries further complicate law enforcement efforts against these transnational criminals.

On the other hand, weak platform liability is also a significant factor in the increasing risk of identity theft. Although Article 16 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions requires electronic system operators to provide reliable and secure systems, this provision remains general and lacks binding technical standards. Empirically, many e-commerce and digital service platforms have not implemented adequate security systems, leaving them vulnerable to data leaks and misuse of user identities. Furthermore, the lack of clear regulations regarding platform liability for user losses further weakens the position of victims.

In terms of evidence, the use of technology in identity theft, such as perpetrator anonymity, the use of the dark web, and cryptocurrency transactions, poses serious obstacles to law enforcement. Although Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions recognizes electronic information as valid evidence, in practice, law enforcement officers still face limitations in digital forensic capabilities and digital transaction tracking. Empirically, this has led to low levels of disclosure of identity theft cases and difficulties in proving perpetrator involvement, thus highlighting the gap between existing legal norms (legal gap) and their implementation in the field (enforcement gap), which underpins the urgency of legal reform in this area.

**Legal Updates in Handling Identity Theft Crimes in Cross-Border E-Commerce Transactions in Indonesia**

Legal reforms in handling identity theft crimes in cross-border e-commerce transactions in Indonesia must begin with the establishment of legal norms that explicitly regulate identity theft as a separate crime within the national legal system. In this context, a reformulation of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions is needed to include a legal definition of identity theft, elements of the crime that include the acquisition of personal data, control of identity, and misuse of identity for unlawful purposes, as well as increased criminal penalties for cross-border transactions or large-scale electronic systems. Concrete actions that can be taken include the preparation of academic papers and drafting laws amending or establishing a special cybercrime law that systematically regulates identity theft as a standalone offense.

Strengthening regulations on personal data protection in the context of cross-border e-commerce is necessary by optimizing the implementation of Law Number 27 of 2022 concerning Personal Data Protection, particularly Article 35 concerning the data controller's obligation to ensure the security of personal data, and Articles 65 and 67 concerning prohibitions and sanctions for misuse of personal data. Concrete actions that need to be taken include the development of implementing regulations governing data security standards for cross-border transactions, mandatory data breach notification, and strengthening oversight mechanisms by competent authorities, so that personal data protection is not only normative but also implementable.

Legal reforms must also include regulating the responsibilities of digital platforms (platform liability) as parties facilitating e-commerce transactions. The provisions in Article 16 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which require electronic system operators

to provide reliable and secure systems, need to be expanded by establishing clear legal responsibilities for failures to protect user data. Concrete actions that can be taken include the creation of regulations requiring platforms to implement certain security standards, provide robust identity verification mechanisms, and be legally responsible for user losses resulting from negligence in maintaining system security.

In cross-border law enforcement, strengthening international cooperation is necessary by harmonizing national laws with global standards. Concrete actions that can be taken include increasing bilateral and multilateral cooperation in information exchange, perpetrator tracking, and extradition, as well as active participation in international forums related to cybercrime. In addition, Indonesia needs to align its national regulations with international practices to facilitate cross-border coordination in handling transnational identity theft.

Legal policy reconstruction must also include the establishment of more effective protection and compensation mechanisms for identity theft victims. Concrete actions that can be taken include establishing a clear compensation scheme for victims, both through civil mechanisms and through compensation obligations by negligent digital platforms. Furthermore, the establishment of a dedicated institution or mechanism to handle complaints and resolve identity theft disputes quickly and efficiently, so that victims are not only left with unrealistic expectations.

Legal reform must adopt a comprehensive approach through the integration of preventive, repressive, and restorative aspects. Concrete actions within the preventive approach include increasing public digital literacy and requiring businesses to implement robust security systems. The repressive approach is implemented through strengthening criminal sanctions and the capacity of law enforcement officers. The restorative approach is realized through victim recovery mechanisms and equitable dispute resolution. Thus, legal reforms are not only normative but also implementable and adaptive to technological developments, thereby ensuring the security of cross-border e-commerce transactions and protecting Indonesia's data sovereignty in a sustainable manner.

## CONCLUSION

Based on the discussion, it can be concluded that Indonesia's positive legal regulations for addressing identity theft in cross-border e-commerce transactions essentially have a normative basis, established through Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection, as well as provisions in the Criminal Code. However, these regulations remain fragmentary, unsystematic, and do not explicitly address identity theft as a separate crime. Furthermore, significant weaknesses exist in both normative and implementation aspects, characterized by the lack of a legal definition of identity theft, weak victim protection, the absence of an effective redress mechanism, and various obstacles to cross-border law enforcement, such as jurisdictional issues, legal conflicts, and limited international cooperation. This situation demonstrates a gap between available legal norms and the effectiveness of their implementation — a legal gap and an enforcement gap — thus rendering existing laws inadequate to address the complexities of identity theft crimes in the digital age.

**REFERENCE**


Adelika, A. N. (2023). Upaya pencegahan terjadinya pencurian data pada e-KTP bagi penduduk pada Dinas Kependudukan dan Pencatatan Sipil Kota Medan. *Jurnal Pengabdian Masyarakat Khatulistiwa*, 124–133.

Alkadrie, S. M. (2023). SIM card dengan identitas palsu: Melanggar hukum atau area kelabu dalam perlindungan data pribadi. *Arus Jurnal Sosial dan Humaniora*, 207–212.

Anugerah, F., & Tantimi. (2022). Pencurian data pribadi di internet dalam perspektif kriminologi. *Jurnal Komunikasi Hukum (JKH)*, 419–435.

Arey, M. S., Hehanussa, D. J., & Salmon, H. C. (2025). Penegakan hukum terhadap kejahatan pencurian data pribadi di media sosial (Facebook). *SANISA: Jurnal Kreativitas Mahasiswa Hukum*, 90–107.

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak pidana cybercrime: Tantangan hukum pidana dalam menanggulangi kejahatan di dunia maya (Desember 2024). *Jurnal Kolaboratif Sains*, 506–511.

Engidaw, A. E., Yu, H., & Zou, W. (2025). Opportunities and challenges in cross-border e-commerce: Strategic management within the legal context of BRI countries—A systematic literature synthesis and future research directions. *Technology Analysis & Strategic Management*.

Fitriani, I., Maulia, I., & Dafira, L. (2025). Perlindungan hukum terhadap konsumen dalam transaksi e-commerce lintas negara. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 1387–1397.

Gabriel, A. (2024). Perlindungan hukum atas data pribadi dalam kasus kebocoran data Pusat Data Nasional Sementara (PDNS) dalam perspektif hukum pidana. *Seminar Nasional: Hukum dan Pancasila*, 33.

Kamisetty, A. (2024). The role of cybersecurity in safeguarding cross-border e-commerce and economic growth. *Asian Business Review*.

Kriswandaru, A. S. (2026). Transformasi hukum nasional dalam era globalisasi digital dan ekonomi berbasis platform. *Judge: Jurnal Hukum*, 1426–1436.

Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Esensi Hukum*, 115–131.

Mahmud, R. (2019). Pencurian identitas: Kategori & kasus. *Cyber Security dan Forensik Digital*, 38–42.

Manurung, M. (2024). Peran marketplace dalam meningkatkan akses pemasaran UMKM di Indonesia. *AB-JOIEC: Al-Bahjah Journal of Islamic Economics*, 74–81.

Nafi'ah, R. (2020). Pelanggaran data dan pencurian identitas pada e-commerce. *Cyber Security dan Forensik Digital*, 7–13.

Nurdiani, I. P. (2020). Pencurian identitas digital sebagai bentuk cyber related crime. *Jurnal Kriminologi Indonesia*, 162.

Purba, Y. O., & Mauluddin, A. (2023). Kejahatan siber dan kebijakan identitas kependudukan digital: Sebuah studi tentang potensi pencurian data online. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial*, 55–66.

Rahayu, D. R., & Padli, N. M. (2023). Kebijakan untuk mencegah pencurian data pribadi dalam media elektronik. *Jurnal Sains dan Teknologi (JSIT)*, 263–266.

Salsabila, F. A., & Ilmih, A. A. (2024). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 176–181.

Sudiantini, D., Ayu, M. P., Aswan, M. C., Prastuti, M. A., & Apriliya, M. (2023). Transformasi digital: Dampak, tantangan, dan peluang untuk pertumbuhan ekonomi digital. *Trending: Jurnal Manajemen dan Ekonomi*, 21–30.

Sulaeman, D., & Kemala, A. P. (2025). Analisis hukum terhadap tindak pidana pencurian

identitas di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 133–148.

Widhaningroem, S. (2024). *Analisis yuridis penyidikan kejahatan e-commerce di Indonesia (Kajian kejahatan penipuan dan pencurian identitas)* [Skripsi, Universitas Muhammadiyah Yogyakarta]. Universitas Muhammadiyah Yogyakarta.