

## Legal Protection for Victims of Digital Scams in Indonesia: A Comparative Study of The Indonesian Anti-Scam Centre (IASC) and The Singapore Police Force Anti-Scam Centre (ASC)

Galuh Putri Setyawati<sup>1\*</sup>, Indah Maulani<sup>2</sup>

<sup>1</sup>E-mail: C100230075@student.ums.ac.id

<sup>2</sup>E-mail: indahmaulani@ums.ac.id

<sup>1,2</sup>Universitas Muhammadiyah Surakarta, Indonesia

\*corresponding author

### Article history:

Received in revised form: 11 July 2026

Acceptance date: 24 September 2026

Available online: 25 October 2026

### Keywords:

Author Guidelines; Consumer Protection; Anti-Scam Centre.

### How to Cite:

Setyawati, G. P., & Maulani, I. (2026). Legal Protection For Victims of Digital Scams in Indonesia: A Comparative Study of The Indonesian Anti-Scam Centre (IASC) and The Singapore Police Force Anti-Scam Centre (ASC). *Al-Risalah Jurnal Ilmu Syariah Dan Hukum*.

<https://doi.org/10.24252/al-risalah.vi.70360>

### License:

Copyright (c) The authors (2026)



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

### Abstract

Consumer protection in the digital era offers numerous benefits but introduces new risks like scams that cause significant financial losses. This study aims to analyze the legal protection for digital scam victims in Indonesia and Singapore and compare the handling mechanisms of the Indonesia Anti Scam Centre (IASC) and the Singapore Police Anti Scam Centre (ASC). This research employs a qualitative normative juridical approach through statutory analysis and comparative study. The findings highlight fundamental differences between the two countries: Singapore's SASC prioritizes preventive measures and law enforcement through an integrated system leveraging AI without focusing its primary mandate directly on recovering victims' funds. Conversely, Indonesia's IASC focuses more on curative efforts such as delaying suspicious transactions and recovering remaining funds, but its implementation is severely hindered by regulatory fragmentation, slow sectoral inter-agency coordination, and the limited jurisdiction of the Financial Services Authority (OJK) in criminal investigations. The main contribution of this research is a specific comparative analysis that maps the legal and institutional gaps in Indonesia, recommending tiered operational integration and measurable responsibility standards to shift the protection orientation from reactive post-loss responses to a coordinated, preventive, and accountable restorative system.

## INTRODUCTION

The development of information and communication technology has fundamentally changed the landscape of economic transactions, creating new opportunities and challenges in consumer protection. Despite providing convenience, the public still needs to increase awareness of the rampant fraud that is growing.<sup>1</sup> In today's digital era, fraud crimes have evolved rapidly along with technological advances, taking advantage of the ease of anonymity, the limitations of people's digital literacy, and the cross-border nature of the internet. Digital fraud, or scam, is a manipulative act that is carried out deliberately to gain personal and group benefits, by harming others.<sup>2</sup>

In the digital landscape, scams include various forms of cybercrime that use digital media as their main tools, ranging from phishing, personal data theft, extortion through *ransomware*, to financial fraud that is increasingly complex and difficult to track.<sup>3</sup> This phenomenon shows the urgency to strengthen the legal apparatus and increase the effectiveness of the implementation of consumer protection. The establishment of an anti-scam center is a strategic step in legal efforts to provide maximum protection to the public from the threat of financial losses caused by digital crime.

Based on a report from the Ministry of Communication and Information of the Republic of Indonesia, during the period 2017 to 2024, there were 572,000 complaints related to online fraud. This number places Indonesia in the ranks of countries with the highest growth rate of cybercrime in Southeast Asia.<sup>4</sup> A similar trend also occurred in Singapore, where the local police recorded 51,501 reports of digital fraud cases throughout 2024, up from 46,563 reports in 2023. The total economic losses caused by scam cases in Singapore in the same year are estimated to reach S\$1.1 billion, equivalent to Rp. 12.1 trillion rupiah.<sup>5</sup>

In Indonesia, the Financial Services Authority (OJK) together with all agencies that are members of the Task Force for the Eradication of Illegal Financial Activities (Satgas PASTI) officially established the Indonesia Anti Scam Center (IASC) on September 22,

---

<sup>1</sup> Asriansyah, M. F. (2023). The Danger of Scam Crime. Taken from DJKN Ministry of Finance: <https://www.djkn.kemenkeu.go.id/kanwil-sumut/baca-artikel/16202/BahayaKejahatan-Scam.html>

<sup>2</sup> Wicaksono, S. R. (2020). *Fraud and Scam in the Digital Era: Concepts and Developments*. CV. Thousand Stars.

<sup>3</sup> Force, S. P. (2024). *Annual Scams and Cybercrime Brief 2024*. Singapore Police Force

<sup>4</sup> Mandra. (2024). The Ministry of Communication and Information Receives Hundreds of Thousands of Online Fraud Complaints. Taken from Radio Republik Indonesia: <https://rri.co.id/nasional/951055/kemenkominfo-terimaratusan-ribu-aduan-penipuan-online>

<sup>5</sup> Wallinda, M. F. (2025). Fraud Victims in Singapore Increase Every Year. Taken from Radio Republik Indonesia: <https://www.rri.co.id/internasional/1354277/korbanpenipuan-di-singapura-meningkat-tiap-tahun>

2024 as a form of collective initiative between institutions in responding to the rise of digital fraud in a more structured and integrated manner. The establishment of the PASTI Task Force itself is based on the Decree of the OJK Board of Commissioners Number 1/KDK.08/2023, which is the implementation of the mandate of Article 247 of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law). This task force consists of 16 ministries and institutions, including the OJK, the Indonesian National Police, the Attorney General's Office, and the Financial Transaction Reporting and Analysis Center (PPATK).

IASC is designated as a national control center in dealing with scam crimes in the financial services sector, to ensure a faster, coordinated, and adaptive response.<sup>6</sup> Its presence is based on the urgent need for a mechanism that is able to respond to the challenges of digital crime complexity effectively and responsively.<sup>7</sup> However, as an institution that is still in the early stages of formation, IASC still faces various challenges in terms of institutional structure, regulatory harmonization, and operational efficiency. This condition reflects that the consumer protection system in Indonesia is not fully integrated and is still running sectorally, which has an impact on the slow handling process and the low rate of recovery of victims' losses. This situation is further exacerbated by the low digital literacy among the public and obstacles in cross-jurisdictional law enforcement.<sup>8</sup>

The study of digital scams can be grouped into several main focuses, namely the characteristics of digital crime, consumer legal protection in electronic transactions, and institutional mechanisms to prevent and deal with fraud. The three focuses are interrelated, but have different pressure points. The study of the characteristics of digital crime highlights the development of fraud modes, the use of technology, and the cross-border nature of cybercrime. The United Nations Office on Drugs and Crime (UNODC, 2024) report, for example, provides context on the development of technology-based fraud and its relationship to organized crime activities in the Southeast Asian region.

---

<sup>6</sup> OJK. (2022). Task Force Profile. Retrieved from Financial Services Authority: <https://ojk.go.id/waspadainvestasi/id/tentang/Pages/Profil-Satgas.aspx>

<sup>7</sup> Hudiyanto. (2024). Consumer Protection Level, PASTI Task Force Conducts Soft Launching of Indonesia Anti-Scam Centre. Taken from the PASTI Task Force for the Eradication of Illegal Financial Activities: [https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP Task Force Must Soft Launch IASC.pdf](https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP%20Task%20Force%20Must%20Soft%20Launch%20IASC.pdf)

<sup>8</sup> United Nation Office on Drugs and Crime. (2024). Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Retrieved from United Nations Office on Drugs and Crime: [https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC\\_Convergence\\_Report\\_2024.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf)

Meanwhile, the study of consumer protection in online transactions, such as Dzuhriyan (2024), is relevant for understanding the legal protection challenges that arise when consumer transactions and interactions take place through electronic systems.

Although there have been the ITE Law, the Criminal Code, and the Consumer Protection Law, the National Criminal Code has not explicitly regulated the victim's right to obtain restitution or compensation quickly. The legal focus is still heavy on the punishment of the perpetrator or the principal crime rather than the financial recovery of the victim. Legal protection for victims is not only related to the prohibition of fraud and the imposition of sanctions on perpetrators, but also includes reporting mechanisms, inter-agency coordination, stopping the flow of funds, tracing transactions, and the possibility of recovering victim losses. Therefore, the analysis of digital scam victim protection needs to connect the legal framework with operational procedures and the sharing of responsibilities between the parties involved.

In terms of consumer protection system comparisons, Indonesia and Singapore offer an interesting perspective, given the differences in the legal systems between the two but have a strategic position in the global economy.<sup>9</sup> Singapore has been implementing an integrated approach through the establishment of the Anti-Scam Centre since 2019, which has proven effective in responding to and tackling various forms of digital crime. The initiative is being carried out under the coordination of the *Inter Ministry Committee on Scams* (IMCS), which involves key agencies such as *the Monetary Authority of Singapore* (MAS), *Singapore Police Force* (SPF) through the dedicated Anti-Scam Command (ASCom), *Infocomm Media Development Authority* (IMDA), and *the Cyber Security Agency of Singapore* (CSA). On the other hand, the Indonesia Financial Services Authority Publication regarding the establishment and implementation of the Indonesia Anti-Scam Center (IASC), including Hudiyanto (2024), provides information about the purpose and initial function of the scam handling center in Indonesia.

Based on data from *the Singapore Police Force*, by 2024, the Anti-Scam Centre has frozen more than 40,900 bank accounts linked to fraudulent activities, as well as recovered more than S\$182 million worth of scam victims. This success is underpinned by a comprehensive regulatory framework, intensive collaboration between law enforcement agencies and the financial sector.<sup>10</sup> As well as the implementation of innovative initiatives

---

<sup>9</sup> Wibowo, D. E. (2024). The Comparison of Indonesian and American Customer Protection Laws: What and How?. *SASI*, 30(4).

<sup>10</sup> Yap, A. (2024). Anti-Scam Centre of the Singapore Police Force: Fighting Scams is a Community Effort. Taken from Singapore Police Force: <https://www.gasa.org/post/anti-scam-centre-of-the-singapore-police-force-fightingscams-is-a-community-effort>

such as the *Shared Responsibility Framework* (SRF), which requires financial institutions and telecommunications companies to implement specific preventive measures against phishing attacks.<sup>11</sup> There are a number of fundamental similarities and differences between the approaches to countering digital fraud implemented by the Indonesia Anti Scam Centre (IASC) and the Singapore Anti Scam Centre (SASC). The IASC in Indonesia has a primary mandate to delay suspicious transactions that are indicated by fraud, identify the parties involved, seek the refund of the remaining victims, and carry out the legal action process against the perpetrators.<sup>12</sup> Meanwhile, the SASC in Singapore also carries out a similar function in terms of stopping and preventing fraudulent activities, as well as law enforcement through the identification of perpetrators. However, unlike the IASC, the SASC does not directly focus on the recovery of victims' funds as part of its main mandate.<sup>13</sup>

These institutional sources are important because they provide information about policies, programs, and practices of handling scams. However, institutional reports fundamentally need to be distinguished from academic research that critically assesses their effectiveness, limitations, and legal implications. The existence of a scam handling center, the use of technology, or the high number of accounts acted upon do not automatically prove that all victims receive the same protection or that the lost funds can be fully recovered. Therefore, institutional reports in this study are used as a source to understand the mechanisms and achievements reported, then analyzed along with the legal basis, institutional authority, handling procedures, and forms of protection available to victims.

A comparative study of consumer protection laws can help explain how different regulatory and institutional frameworks affect the implementation of consumer rights. Wibowo (2024), for example, discusses a comparison of consumer protection laws between Indonesia and the United States. The study is relevant as a reference for a comparative approach in consumer protection law, but cannot be directly used to

---

<sup>11</sup> Derry, L. (2025). Singapore's Scam Surge Strategy: What Enterprises Must Do Now Under the New Shared Responsibility Framework. Retrieved from Memcyco: <https://www.memcyco.com/singapore-shared-responsibility-framework>

<sup>12</sup> Hudiyanto. (2024). Consumer Protection Level, PASTI Task Force Conducts Soft Launching of Indonesia Anti-Scam Centre. Taken from the PASTI Task Force for the Eradication of Illegal Financial Activities: [https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP Task Force Must Soft Launch IASC.pdf](https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP%20Task%20Force%20Must%20Soft%20Launch%20IASC.pdf)

<sup>13</sup> Domnic Dass. (2021). Dedication To Disrupt And Prevent Scam Operations. Taken from Singapore Police Force: [https://www.police.gov.sg/Media-Room/PoliceLife/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-AgainstScams#:~:text=The Anti-Scam Centre \(ASC\) was set up,Police's nerve centre for investigating scam-related crimes](https://www.police.gov.sg/Media-Room/PoliceLife/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-AgainstScams#:~:text=The%20Anti-Scam%20Centre%20(ASC)%20was%20set%20up,Police's%20nerve%20centre%20for%20investigating%20scam-related%20crimes)

conclude the difference in the mechanism of handling scams between Indonesia and Singapore because the object of comparison is different. In the context of Indonesia and Singapore, the comparison needs to be directed at aspects that are truly related to the protection of victims of digital scams. These aspects include the position and authority of the handling agency, the relationship between the scam handling center and law enforcement officials, coordination with financial and telecommunication service providers, the speed of response to reports, the procedure for blocking or withholding funds, and the legal basis for the division of responsibility if losses occur. Comparisons also need to distinguish between preventive measures, termination of transactions, criminal investigations, and recovery of losses.

These four things are interrelated, but they are not identical functions and are not always under the authority of a single institution. With this framework, Singapore's experience is not treated as a model that can be transferred directly to Indonesia. Differences in institutional structure, legal authority, characteristics of the financial system, and responsibility arrangements need to be taken into account before a practice is deemed relevant to be adapted. A comparative approach thus aims not only to identify systems that appear to be more advanced, but also to assess the legal and institutional conditions that allow a mechanism to operate as well as the limits of its application in the Indonesian context.

Based on this group of literature, this study places the issue of digital scam victim protection at the intersection of legal norms, institutional design, and the implementation of case handling mechanisms. The literature on digital crime provides context on the development of threats; consumer protection studies provide a basis for assessing the position and rights of consumers; while institutional reports explain the policies and practices of handling implemented. However, the three source groups need to be synthesized through a comparative framework that consistently assesses the relationship between institutional authority, handling coordination, cessation of funds, and opportunities to recover victims' losses.

The position of this study lies in the comparison of the digital scam victim protection mechanism in Indonesia and Singapore with the IASC and the Anti-Scam Centre mechanism in Singapore as an institutional focus. The comparison was made not only to describe the two handling centres, but to examine how the different legal frameworks and coordination between parties affect the stages of case handling and the forms of protection that victims can access. A comparative study with the Singapore Anti Scam Centre (SASC) is important to adopt an integrated system, cutting-edge technology (AI/RPA), and a *Shared Responsibility Framework* to strengthen the newly operational

Indonesia Anti Scam Centre (IASC). SASC Singapore operates with an integrated, fast, and technologically advanced system, while IASC in Indonesia still faces challenges of inter-agency coordination and slow response times. Although IASC has successfully blocked accounts and returned funds, the comparative study helps to speed up legal procedures so that the restoration of the rights of material and immaterial victims is maximized. This study aims to find out the legal arrangements for the protection of consumers who are victims of digital scams in Indonesia and to find out the comparison of the mechanism for handling scam victims between the Indonesia Anti Scam Centre (IASC) and the Singapore Anti Scam Centre (SASC).

Thus, the contribution of this research is directed at the preparation of a comparative analysis that connects the legal basis, institutional authority, operational procedures, and orientation of victim loss recovery. The results of the comparison are expected to identify relevant practices to consider in Indonesia as well as explain the legal and institutional prerequisites required in their implementation. This position also allows the research to provide more targeted recommendations rather than simply suggesting technology adoption or improved coordination in general.

## **METHODS**

This research method uses a type of normative juridical legal research, which is legal research conducted by examining literature materials or secondary data, also known as doctrinal research.<sup>14</sup> The approach used in this study is a normative juridical approach with a *Comparative Approach*. The *Comparative Approach* approach is carried out by comparing laws (*comparative law*) which often compare between countries with the Civil Law system (such as Indonesia) and *Common Law* countries (such as the UK/US).<sup>15</sup> The legal material consists of Law Number 8 of 1999 concerning Consumer Protection, Law of the Republic of Indonesia Number 1 of 2024 as the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector. In addition, this study also contains a comparative study with the Singapore legal system, with the aim of examining the effectiveness and governance of the establishment of the Indonesia Anti Scam Centre (IASC) compared to the Singapore Anti Scam Centre (SASC), which is known to have a systematic approach and has proven to be successful. Regulations that

---

<sup>14</sup> Soerjono Soekanto and Sri Mamuji (2013). *Normative Law Research: A Brief Review*. Jakarta: Raja Grafindo Persada, p. 13.

<sup>15</sup> Peter Mahmud Marzuki (2013), *Legal Research* (Revised edition), Jakarta: Kencana Prenada Media Group, p.133

are used as a reference in the Singapore context include *the Computer Misuse Act (CMA)*, *Cybersecurity Act 2018*, *Shared Responsibility Framework (SRF)*, *Personal Data Protection Act (PDPA)*, and *Electronic Transactions Act (ETA)*.

## RESULTS AND DISCUSSION

### 1. Legal Arrangements for the Protection of Consumers Who Are Victims of Digital Scams in Indonesia

The role of the government and the industrial sector has become very strategic in building a digital ecosystem that is safe, transparent, and fair for consumers. The government bears the main responsibility in ensuring consumer protection from harmful and unethical business practices. One of the main instruments used is through the establishment of a strict legal and regulatory framework, which not only establishes the rights and obligations of consumers, but also provides proportionate sanctions for business actors who are proven to have committed violations.<sup>16</sup> This effort aims to create a balance between the interests of consumers and business actors, as well as encourage the creation of business practices with integrity and responsibility in the digital economy era. The development of information and communication technology has fundamentally changed the landscape of economic transactions, creating new opportunities and challenges in consumer protection. The crime of digital fraud or scams is currently undergoing rapid evolution in line with technological advancements, taking advantage of the ease of anonymity, limited digital literacy of the community, and the cross-border nature of the internet. As a manipulative act that is deliberately carried out for personal gain by harming others, scams in the digital landscape include phishing, personal data theft, extortion through ransomware, and increasingly complex financial fraud.

In order to respond to the rampant threat of crime, the law in Indonesia implements several main regulatory instruments that function as pillars of consumer protection, both through preventive (prevention) and repressive (law enforcement) approaches.

#### a. Law Number 8 of 1999 concerning Consumer Protection (UUPK)

This law is the main pillar that explicitly guarantees the right of consumers to obtain accurate, honest, and non-misleading information about goods and/or services, including in the context of digital transactions. In relation to preventive protection, the UUPK emphasizes the importance of transparency through the obligation of service providers to convey clear information, including privacy policies and data protection

---

<sup>16</sup> Riana, P. (2024). *Anti-Fraud Guide: Consumer Strategies to Avoid Fraud and Fraudulent Business Practices*. Surabaya. CV. Garuda Mas Sejahtera.

mechanisms implemented by business actors. In addition, this regulation provides protection for consumer privacy in terms of collection, processing, and use of personal data. Meanwhile, the repressive function is shown when business actors or scam actors manipulate information, where the misuse of the information is categorized as a form of violation of the principles of consumer protection as stipulated in the UUPK, which can lead to the imposition of proportionate sanctions for parties proven to have committed violations. In Indonesia, Law Number 8 of 1999 concerning Consumer Protection,

The Consumer Protection Law affirms the right of consumers to obtain honest and correct information about goods/services, including in digital transactions, as well as provides the right to privacy in the collection, use, and processing of personal information by goods/service providers. In addition, recognizing electronic transactions, the Consumer Protection Law regulates consumer rights in this context, including providing clear and comprehensive information about electronic transactions, including privacy policies implemented by service providers.<sup>17</sup>.

In Indonesia, there are three main regulatory pillars that have a vital role in providing legal protection for consumers in the midst of the dynamics of the digital era, namely Law Number 8 of 1999 concerning Consumer Protection, Law of the Republic of Indonesia Number 1 of 2024 as the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), and Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law). These three laws form a comprehensive legal basis in dealing with contemporary challenges such as the rise of online fraud cases (scams).

The Consumer Protection Law explicitly guarantees consumers' rights to obtain accurate, honest, and non-misleading information about goods and/or services, including in the context of digital transactions. In addition, this law also provides protection for consumer privacy in terms of the collection, processing, and use of personal data by business actors. In relation to electronic transactions, the Consumer Protection Law emphasizes the importance of transparency through the obligation of service providers to convey clear information, including privacy policies and data protection mechanisms implemented. Meanwhile, the ITE Law and the P2SK Law strengthen aspects of law enforcement and supervision against the misuse of information technology and illegal financial activities, so that these entire frameworks complement each other in creating a more resilient and adaptive consumer protection system in the digital era.

---

<sup>17</sup> Yuyut, P. (2024). The Dynamics of Consumer Legal Protection in the Digital Era: Legal Analysis of E-Commerce Practices and Consumer Data Protection in Indonesia. *Journal of Legal Interpretation*, Volume 5 Number 1, 907.

In the context of scam practices, consumers often do not obtain adequate information about the risks, product specifications, and payment schemes offered. Digital fraud continues to evolve with increasingly complex and disguised *modus operandi*, so that many consumers are trapped without realizing that they have become victims. This situation reflects a serious gap in the implementation of law enforcement, especially regarding the obligation of information transparency that should be guaranteed by laws and regulations. Misuse of information by scammers to manipulate and deceive consumers is a form of violation of the principles of consumer protection as stipulated in Law Number 8 of 1999 concerning Consumer Protection. The lack of control and verification of circulating information, as well as weak digital supervision, makes legal protection mechanisms for consumers less effective in counteracting increasingly rampant fraudulent practices.<sup>18</sup>

Related Articles on Digital Scams and Consumer Protection:

| Article                 | Substance                                                                                                     | Protection aspects                                           |
|-------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Article 4 Paragraph (1) | Consumers have the right to security, safety, and comfort in using goods/services                             | Preventive<br>Ensuring the security of digital transactions  |
| Article 4 Paragraph (2) | Consumers have the right to receive true, clear, and honest information about the condition of goods/services | Preventive<br>Prevent false information in scams             |
| Article 28              | Prohibit the inclusion of standard clauses that are detrimental to consumers                                  | Preventive<br>Protect against non-transparent provisions     |
| Article 45              | Consumers who suffer losses can file a lawsuit through the district court                                     | Repressive<br>Legal mechanisms for victims                   |
| Article 46              | Lawsuits can be filed individually or by consumer groups                                                      | Repressive –<br>acceleration of the collective legal process |

#### b. Electronic Information and Transaction Law (ITE Law)

Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law) is present as a strategic legal foundation in strengthening consumer protection in the digital realm, especially in the face of increasingly prevalent fraudulent practices in electronic transactions. This law is designed to provide firm legal certainty for cybercriminals who use electronic media as a means to commit criminal acts, including

<sup>18</sup> Jennifer, C. (2024). Legal Protection for Consumers Who Are Victims of Illegal Investment Companies Based on Multi-Level Marketing. *USM Law Rivew Journal*, Volume 7(3).

scams. One of the crucial provisions in the ITE Law regulates the responsibility of electronic system operators (PSEs), who are required to ensure that all transaction activities on their platforms take place in accordance with legal provisions and are free from the spread of false information that can harm consumers.<sup>19</sup>

| Article                      | Substance                                                                                      | Sanctions                                                      | Aspects    |
|------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------|------------|
| Article 28<br>Paragraph (1)  | Spreading false and misleading news that results in consumer losses in Electronic Transactions | Maximum imprisonment of 6 years and/or a fine of IDR 1 billion | Repressive |
| Article 45A<br>Paragraph (1) | Sanctions for Article 28 Paragraph (1)                                                         | Maximum imprisonment of 6 years and/or a fine of IDR 1 billion | Repressive |

The very crucial repressive instrument is contained in Article 28 paragraph (1) of the ITE Law which normatively ensnares the actions of scammers, by stating that "Everyone deliberately and without the right spreads false and misleading news that results in consumer losses in electronic transactions". However, the application of this article has been criticized because the law enforcement still tends to be repressive-reactive (the law only runs after the consumer loses) and has not fully accommodated the needs of victim restitution quickly, thus leaving a gap in regulation regarding the mechanism for reimbursement of victims of digital scams.

However, in practice, the implementation of this article still faces serious challenges, the criminal aspect of the perpetrator rather than the recovery of victim losses related to the legal protection provided is still repressive and does not fully accommodate the needs of victim restitution quickly and effectively, then this condition shows that there is a regulatory vacuum regarding the mechanism for reimbursement of digital scam victims. Criticism of the ITE Law also arises because of its repressive and reactive approach, where legal action is generally taken after consumers have suffered losses, rather than through systematic prevention efforts.<sup>20</sup>

c. Criminal Code (Criminal Code / Law No. 1 of 2023)

Although Indonesia already has the ITE Law and the UUPK, the handling of the main crime of fraud in general still relies on the Criminal Code. Through legal reforms in the National Criminal Code (Law No. 1 of 2023), law enforcement against cybercrime

<sup>19</sup> Irfan, R. (2024). Legal Aspects of Digital Consumer Protection. *Civilia: Journal of Legal Studies and Civic Education*, Volume 3(2).

<sup>20</sup> Syadid, J. A. (2025). Comparison of Cybercrime Laws Between Indonesia and Singapore. *Journal of Law and Citizenship*, Volumes 10, 11.

perpetrators is directed to strict criminal sanctions. However, in the context of consumer protection, the legal approach in the National Criminal Code is considered to be heavy on the repressive aspect, namely focusing on punishing the perpetrator or the principal crime rather than the financial recovery of consumers. The National Criminal Code does not explicitly regulate the right of victims to obtain restitution or compensation quickly from material losses due to *digital* scams. As a result, it is still difficult for victims to get complete justice and instant recovery of losses in the field. Law No. 1 of 2023 concerning the National Criminal Code officially takes effect on January 1, 2026, replacing the old Criminal Code. This regulation is here as an answer to the complexity of the increasingly sophisticated digital crime mode

| Article     | Substance                                                  | Sanctions                                                                 | Aspects    |
|-------------|------------------------------------------------------------|---------------------------------------------------------------------------|------------|
| Article 492 | Scams with fake names/positions, tricks, a network of lies | Maximum imprisonment of 4 years or a fine of category V (IDR 500 million) | Repressive |
| Article 493 | Minor fraud (loss < IDR 250,000)                           | Maximum imprisonment of 3 months or a fine of IDR 900,000                 | Repressive |

Article 492 of Law No. 1 of 2023 (new Criminal Code) reads: "Every person with the intention of unlawfully benefiting himself or others by using a false name or position, using trickery or a series of lies, moving people to hand over an item, giving debts, making a confession of debt, or writing receivables, shall be convicted of fraud with a maximum prison sentence of 4 years or a maximum fine of category V, which is IDR 500,000,000".

In essence, fraudsters can be charged with Article 378 of the Criminal Code or Article 492 of Law 1/2023 concerning the new Criminal Code which will take effect in 2026, but can also be charged with Article 28 paragraph (1). Article 45A paragraph (1) of Law 1/2024 if fraud is committed online. Perpetrators of music concert ticket fraud can be charged with Article 378 of the Criminal Code or Article 492 of Law 1/2023, but can also be charged with Article 28 paragraph (1) jo. Article 45A paragraph (1) of Law 1/2024 if fraud is committed online. The criminalization policy in the New Criminal Code reflects a paradigm shift from retributive justice to corrective and restorative justice through the transformation of fine sanctions into a category system (category V to Rp.500,000,000,-) as well as the expansion of legal subjects that include corporations. Article 492 of the New Criminal Code has juridical flexibility that is able to reach the evolution of online fraud modes through the redefinition of the elements of "series of lies" and "deception" into the form of data manipulation and electronic systems. Article 492 of Law No. 1 of 2023 (new

Criminal Code) has the flexibility to reach online fraud modes Comparison with the old Criminal Code (Article 378):

- 1) Old Criminal Code: Criminal Penalty of IDR 900,000
- 2) New Criminal Code: Criminal Penalty of Category V Fine (IDR 500 million)
- 3) Legal Subject: The new Criminal Code covers corporations
- 4) Coverage: Includes digital transactions

The criminalization policy in the New Criminal Code reflects a paradigm shift from retributive justice to corrective and restorative justice through the transformation of fine sanctions into a categorical system. Article 492 of the New Criminal Code has juridical flexibility that is able to reach the evolution of online fraud modes through the redefinition of the elements of "series of lies" and "deception" into the form of data manipulation and electronic systems.

d. Financial Services Authority (OJK) and Financial Sector Regulations

OJK actively regulates and supervises technology financial platforms to ensure transaction security and consumer protection

| Regulation          | Year | Substance                                                                                | Aspects                 |
|---------------------|------|------------------------------------------------------------------------------------------|-------------------------|
| POJK No. 22 of 2023 | 2023 | Consumer and Community Protection in the Financial Services Sector                       | Preventive & Repressive |
| POJK No. 40 of 2024 | 2024 | Information Technology-Based Joint Funding Services                                      | Preventive              |
| POJK No. 12 of 2024 | 2024 | Implementation of Anti-Fraud Strategy for Financial Services Institutions (POJK SAF LJK) | Preventive & Repressive |

Related Articles/Clauses in POJK No. 22 of 2023:

This POJK replaces POJK No. 6/POJK.07/2022 and improves several other POJK. The substance of strengthening consumer protection includes:

- 1) Information transparency obligations  
PUJK is obliged to provide complete and clear information about products/services
- 2) Personal data protection  
Obligation to ensure information system security and cyber resilience
- 3) Complaint mechanism  
Adjusted complaint service period for PUJK
- 4) Transparency of interest and fees.  
Minimizing the risk of non-transparent flower practices

POJK No. 12 of 2024 concerning Anti-Fraud Strategy:

This regulation requires Financial Services Institutions (LJK) to develop and implement anti-fraud strategies with 4 pillars:

- 1) Prevention
- 2) Detection
- 3) Investigation, reporting, and sanctions
- 4) Monitoring, evaluation, and follow-up

The types of acts classified as fraud consist of corruption, misuse of assets, fraud in financial statements, fraud, leaking confidential information, and/or other actions that can be likened to fraud. OJK has established a PASTI Task Force to combat misuse of online loan collection practices and developed the APPK platform as a regulatory tool for complaints. OJK Issues New Consumer Protection Rules with POJK Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector

Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law) is one of the strategic legal pillars in strengthening the national financial ecosystem, as well as the main juridical basis for the establishment of the Indonesia Anti Scam Center (IASC). This regulation not only emphasizes the establishment of a more inclusive and formal financial services sector, but also focuses on strengthening consumer protection aspects and the integrity of the national financial system.

Article 5 letter c emphasizes that the main objective of the development of the financial services sector is to encourage stable and sustainable national economic growth through the strengthening of an efficient, healthy, and competitive financial services sector. Meanwhile, Article 6 letter e explicitly regulates the functions of the financial authority in carrying out supervision and regulation in order to ensure the security, stability, and protection of consumers in the financial sphere. This provision is the basis for the authority for the Financial Services Authority (OJK) to carry out the supervisory function and handle and prevent criminal acts in the financial sector. Thus, the OJK has legal standing in initiating various preventive and responsive measures, including rapid intervention in scam cases, blocking suspicious accounts, identification of parties involved, and intensive coordination with law enforcement officials such as the Indonesian National Police. Furthermore, Article 247 of the P2SK Law specifically regulates the establishment of the Task Force for the Eradication of Illegal Financial Activities (Satgas PASTI) chaired by the OJK, with the main mandate of preventing and dealing with unlawful practices in the collection of public funds and the management of

illegal investments, which also serves as an operational framework for IASC in dealing with cybercrime in the financial services sector.

The establishment of the Indonesia Anti-Scam Center (IASC) was motivated by the urgent need for a fast and integrated response system to the increasing cases of fraud in the financial services sector. IASC acts as a coordination node between financial service providers to accelerate the process of handling digital financial crime reports, focusing on delaying suspicious transactions, blocking accounts indicated to be involved in fraud, identifying actors involved, efforts to recover victims who can still be rescued, and assistance in the law enforcement process. In its implementation, IASC receives broad support from various stakeholders such as banking associations, payment system service providers, and e-commerce platforms, which together form a digital defense ecosystem against financial crime.<sup>21</sup>

## **2. Comparison of Scam Victim Handling Mechanisms between Indonesia Anti Scam Centre (IASC) and Singapore Police Anti Scam Centre (ASC).**

Singapore implements a multi-layered and sophisticated approach to consumer protection, leveraging digital intelligence, user behavior analysis, and fund flow risk evaluation to detect and prevent fraud early. Cutting-edge technologies such as Artificial Intelligence (AI) play a central role, including the SATIS (*Suspicious Activity Transaction Identification System*) system and facial recognition technology used to identify suspicious patterns and modus operandi often used by digital criminals. On the regulatory side, Singapore strengthens the position of consumers through the implementation of the *Shared Responsibility Framework* (SRF), which expressly establishes the obligations of banks and telecommunications operators in handling phishing cases. Within this framework, institutions that neglect to carry out their responsibilities are required to compensate for losses incurred due to illegal transactions, thereby adding a concrete layer of legal and operational protection for the community.<sup>22</sup>

A comparison of digital scam victim protection mechanisms in Indonesia and Singapore shows that the effectiveness of consumer protection is not only determined by the existence of special institutions or the sophistication of the technology used, but also by the relationship between institutional authority, the certainty of report handling

---

<sup>21</sup> Hudiyanto. (2024). Consumer Protection Level, PASTI Task Force Conducts Soft Launching of Indonesia Anti-Scam Centre. Taken from the PASTI Task Force for the Eradication of Illegal Financial Activities: [https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP Task Force Must Soft Launch IASC.pdf](https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP%20Task%20Force%20Must%20Soft%20Launch%20IASC.pdf)

<sup>22</sup> Vienna, V. (2025). Singapore needs a multi-layered strategy to fight fraud. Retrieved from Banking & Finance: <https://asianbankingandfinance.net/indonesian/exclusive/singapura-membutuhkanstrategi-berlapis-untuk-melawan-penipuan>

procedures, the exchange of information, and the division of responsibilities between parties. In Indonesia, the Indonesia Anti Scam Centre (IASC), which is part of the Financial Services Authority (OJK) coordination ecosystem, acts as a center for receiving and coordinating fraud reports in the financial sector, especially to support transaction tracing, blocking accounts indicated for fraud, and efforts to rescue funds that are still available. Meanwhile, handling scams in Singapore involves coordination between law enforcement agencies, financial authorities, and authorities that handle communications and cybersecurity.

The Singapore Police Force (SPF), through the Anti-Scam Centre (ASC) and Anti-Scam Command (ASCom), has a role in handling and investigating criminal acts, while the Monetary Authority of Singapore (MAS) plays a role in overseeing the financial sector. This difference suggests that victim protection requires a nexus between transaction safeguarding mechanisms and law enforcement authorities. When these functions run through interconnected procedures, information about recipient accounts, suspicious transactions, and suspected criminal acts can be followed up in a more targeted manner. Conversely, if the coordination process still relies on communication and follow-up between separate agencies, there is a risk of delays when fraudulent funds are transferred through multiple accounts or financial service providers.

These institutional differences need to be understood in the context of the division of authority in each country. In Indonesia, the OJK has the authority to regulate and supervise the financial services sector, while the investigation and investigation of criminal acts is within the realm of law enforcement officials in accordance with the provisions of laws and regulations. Therefore, the existence of the IASC does not in itself eliminate the need for coordination with the police, financial service providers, and other relevant parties. The challenge is not simply because there are many institutions involved, but rather how each institution obtains the information needed, knows the actions it is responsible for, and carries out those actions without unnecessary delay. Singapore also involves a number of institutions, but the division of functions between law enforcement and financial sector supervision provides a basis for handling that links criminal aspects to transaction security.

Thus, the main lesson for Indonesia is not to unite all authorities in one institution, but to build a coordination mechanism that has a division of responsibilities, data exchange standards, escalation paths, and clear handling deadlines. This model is more realistically applied than making comprehensive institutional changes, because it can strengthen existing coordination without ignoring the limits of the authority of each institution. From a technological perspective, the differences between the two countries

also need to be seen based on the function of technology in the overall victim protection process, not just the number or sophistication of the devices used. The use of digital systems in handling scams can support the identification of accounts that are repeatedly reported, analysis of unusual transaction patterns, matching information from a number of reports, and the delivery of warnings to potential victims.

In Singapore, the use of reporting channels, monitoring mechanisms, and scam prevention support devices is part of an approach that links preventive measures with handling by the authorities. Meanwhile, the strengthening of technology in Indonesia through the IASC needs to be directed so that the reports received are not only administrative data, but can also be used to recognize the linkage between cases and speed up the delivery of information to the authorities. The use of artificial intelligence (AI) and robotic process automation (RPA) can be considered to help the process, but their implementation does not automatically guarantee successful handling. Data quality, system interoperability, information security, personal data protection, and the ability of officers to follow up on analysis results remain decisive factors.

Therefore, Indonesia needs to prioritize data integration and automation of basic processes first before developing more complex prediction systems. Technology should be positioned as a means to accelerate action by authorized agencies, not as a substitute for human judgment, evidence checks, or legal procedures. These different approaches have direct implications for responses to victim reports. In the case of digital scams, time is of paramount importance because funds can be moved quickly from the first recipient's account to another, withdrawn in cash, or diverted through various payment services. Therefore, an effective protection mechanism needs to distinguish between receipt of reports, initial verification, submission of information to financial service providers, safeguarding of funds, and follow-up by law enforcement.

Each stage has different purposes and authority, so it is not appropriate if the entire process is considered complete simply because a report has been received or the account has been flagged as suspicious. Singapore's experience shows the importance of interconnectedness between reports, transaction information, and investigative actions. In the Indonesian context, IASC can be strengthened through tiered response procedures, for example by prioritizing reports that show new transactions and have verifiable recipient account information. Furthermore, reports need to obtain a tracking number, a monitoring handling status, and information about actions that have been taken and the next steps that the victim needs to take. Response time standards also need to be differentiated based on the type of action and the level of urgency, so as not to give the impression that all reports can be completed in the same time.

This approach will clarify the accountability of handling while reducing the uncertainty experienced by victims after reporting losses. The recovery aspect of funds shows that victim protection cannot be measured only by the number of blocked accounts or reports received. Blocking is an important step to hinder the movement of funds, but it is not synonymous with successfully returning money to victims. Funds that have been successfully secured still need to be traced, verified for ownership, and processed through mechanisms in accordance with legal provisions. If funds have been moved to another account, withdrawn, or diverted outside of an accessible payment system, the chances of recovery may be limited. Therefore, the evaluation of the Indonesian and Singapore mechanisms needs to distinguish at least three outcomes, namely funds that have been successfully blocked or secured, funds that have been returned to victims, and funds that have not been recoverable.

This distinction is important so that operational success is not equated with substantive restoration of victims' rights. In the Indonesian context, the IASC can be strengthened through an ongoing fund tracking mechanism, transparent claims verification procedures, coordination between parties when funds pass through multiple accounts, and the provision of clear information about the possibilities and limitations of refunds. In addition, there needs to be a procedure in place that explains how victims can follow up on reports when funds have been secured but have not been returned. Thus, the recovery of funds is placed as a series of measurable processes, not just an automatic consequence of account blocking.

The difference in victim protection between Indonesia and Singapore is also related to the regulation of the liability of financial and telecommunications service providers. In Indonesia, the handling of scams involves provisions that govern consumer protection, supervision of the financial services sector, electronic transactions, and law enforcement. However, the existence of a number of rules does not by itself form a uniform mechanism for the division of responsibility for each case. Meanwhile, Singapore developed the Shared Responsibility Framework (SRF) which establishes certain obligations for financial institutions and telecommunication service providers within the regulated scope, especially related to phishing prevention. This framework is important because it places prevention as a responsibility that is not fully imposed on users. However, SRF cannot be interpreted as a universal obligation for all service providers to compensate for any losses caused by all types of scams.

Its application depends on the scope of the provisions, the type of incident, the fulfillment of each party's obligations, and the conditions set out in the framework. For Indonesia, the lesson that can be learned is the need to formulate clearer standards of

liability when losses occur due to failure to meet security obligations or pre-established handling procedures. The development of such policies needs to be preceded by mapping the types of scams, identifying risks that can be controlled by each party, and determining liability standards that can be objectively assessed. In this way, the division of responsibility can improve victim protection without ignoring the fact that not all fraud occurs due to the negligence of service providers. In the recovery of victims' assets, ASCom Singapore managed to recover more than S\$182 million in 2024, while IASC Indonesia's asset recovery data is still limited, with IDR 129.1 billion in funds blocked from the total loss of IDR 1.2 trillion reported until March 2025. Both countries recognize the importance of public education, but Indonesia's current condition faces constraints due to the low digital literacy of its people.<sup>23</sup> Singapore has implemented technology solutions such as the ScamShield application and the SATIS AI analytics system, while Indonesia through IASC is working to improve the use of technology and propose an integrated National Hotline. The blocking rate of illegal entities/content is high in both countries, but the dynamic nature of scams still makes it difficult to do so. Singapore recorded a growth in scam cases of +10.6% (2023-2024), and in Indonesia, consumer reports of losses due to scams increased from 19% (2023) to 23% (2024). Singapore's IMDA blocked 117 million calls & 50 million SMS scams in 2024, and SPF blocked more than 44,900 scam-related websites in the same year.<sup>24</sup>

Based on these comparisons, the adoption of Singapore's policies in Indonesia needs to be selective and gradual. The first priority is to strengthen IASC's operational coordination with financial service providers and law enforcement officials through standardized information exchange procedures, clear responsible persons, and standard response times for urgent action. The second priority is to develop a case reporting and tracking system that allows victims to know the status of reports without having to repeat all information to each institution. The third priority is to gradually build data integration and risk analysis tools, ensuring that the use of technology is supported by data governance, information security, and oversight mechanisms. Once the foundation is established, Indonesia can consider more measurable responsibility-sharing arrangements for banks and telecommunication service providers, including default assessment criteria, complaint resolution procedures, and transparent redress

---

<sup>23</sup> Kholid, R. (2025). PASTI Task Force urges extra vigilance against fraud ahead of Eid. Taken from IDN Financials: <https://www.idnfinancials.com/news/53358/satgas-pastiurges-extra-vigilance-against-fraud-ahead-of-eid>

<sup>24</sup> Tech for Good Institute. (2025). Building Resilience against Scams and Fraud: Spotlight on Indonesia. Taken from Tech for Good Institute <https://techforgoodinstitute.org/blog/event-highlights/building-resilience-againstscams-and-fraud-spotlight-on-indonesia/>

mechanisms. This phased approach is more realistic than directly copying the entire Singapore system, as the two countries differ in scale of territory, institutional capacity, financial services industry structure, and digital literacy conditions. Adoption success also needs to be measured through results-oriented indicators, such as the time between reports and safeguarding measures, the proportion of funds successfully returned versus the funds secured, the clarity of report status, and the consistency of inter-agency follow-up.

Thus, the comparison of Indonesia and Singapore shows that the differences in digital scam victim protection mechanisms are not solely derived from the level of technological advancement, but also from how authorities, procedures, and responsibilities are structured to produce interconnected actions. The strength of Singapore's approach lies in the interconnectedness between law enforcement coordination, financial sector supervision, prevention, and the regulation of relevant stakeholders' liability. Meanwhile, strengthening IASC in Indonesia needs to be directed at increasing inter-agency interoperability, accelerating responses to urgent reports, transparency of the fund recovery process, and developing accountability standards that can be applied consistently. Therefore, the goal of comparative learning is not to make Singapore a fully copied model, but to identify principles that can be adapted to Indonesia's legal framework and institutional capacity. This approach is expected to shift the orientation of protection from response after a loss has occurred to a more coordinated, preventive, accountable, and victim-rights recovery-oriented system.

## CONCLUSION

The applicable regulations show that legal protection for consumers who are victims of digital scams in Indonesia is still hampered by regulatory fragmentation and lack of synchronization between agencies. Although Law No. 8 of 1999 on Consumer Protection and Law No. 1 of 2024 on Information and Electronic Transactions provide an important legal framework, their implementation is still weak, especially since the Financial Services Authority (OJK) does not have jurisdiction to investigate crimes. A comparison of the handling mechanisms between the Indonesia Anti Scam Centre (IASC) and the Singapore Anti Scam Centre (SASC) shows significant differences in the approach taken by the two countries. SASC in Singapore operates with an integrated and coordinated system, utilizing advanced technologies such as Robotic Process Automation (RPA) and Artificial Intelligence (AI) to proactively detect and prevent scams, and has a clear regulatory framework through the Shared Responsibility Framework (SRF). In contrast, IASCs in Indonesia still face challenges in terms of inter-agency coordination and slow

response times, as well as the OJK's lack of jurisdiction in criminal investigations. This suggests that Indonesia needs to adopt best practices from Singapore, including increased inter-agency collaboration and technology utilization, to strengthen scam handling mechanisms and protect consumers more effectively.

## REFERENCES

- Asriansyah, M. F. (2023). The Dangers of Scam Crimes. Taken from DJKN Ministry of Finance: <https://www.djkn.kemenkeu.go.id/kanwil-sumut/baca-artikel/16202/BahayaKejahatan-Scam.html>
- Dass, D. (2021). The Anti-Scam Centre: A collaborative approach against scams. Singapore Police Force. <https://www.police.gov.sg/media-hub/police-life/2021/11/the-anti-scam-centre---a-collaborative-approach-against-scams>.
- Derry, L. (2025). Singapore's Scam Surge Strategy: What Enterprises Must Do Now Under the New Shared Responsibility Framework. Retrieved from Memcyco: <https://www.memcyco.com/singapore-shared-responsibility-framework>
- Domnic Dass. (2021). Dedication to disrupt and prevent scam operations. Taken from Singapore Police Force: [https://www.police.gov.sg/Media-Room/PoliceLife/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-AgainstScams#:~:text=The Anti-Scam Centre \(ASC\) was set up,Police's nerve centre for investigating scam-related crimes](https://www.police.gov.sg/Media-Room/PoliceLife/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-AgainstScams#:~:text=The Anti-Scam Centre (ASC) was set up,Police's nerve centre for investigating scam-related crimes)
- Dzuhriyan, A. R. (2024). Consumer Legal Protection in Online Transactions: Challenges and Opportunities in Indonesia's Digital Economy. *Justice Voice*, Volume 3(1).
- Force, S. P. (2024). Annual Scams and Cybercrime Brief 2024. Singapore Police Force
- Hudiyanto. (2024). Consumer Protection Level, PASTI Task Force Conducts Soft Launching of Indonesia Anti-Scam Centre. Taken from the PASTI Task Force for the Eradication of Illegal Financial Activities: <https://ojk.go.id/id/berita-dan-kegiatan/infoterkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-LakukanSoft-Launching-IASC/SP-Satgas-Pasti-Soft-Launching-IASC.pdf>
- Irfan, R. (2024). Legal Aspects of Digital Consumer Protection. *Civilia: Journal of Legal Studies and Civic Education*, Volume 3(2).
- Jennifer, C. (2024). Legal Protection for Consumers Who Are Victims of Illegal Investment Companies Based on Multi-Level Marketing. *USM Law Rivew Journal*, Volume 7(3).
- Kholid, R. (2025). PASTI Task Force urges extra vigilance against fraud ahead of Eid. Taken from IDN Financials: <https://www.idnfinancials.com/news/53358/satgas-pastiurges-extra-vigilance-against-fraud-ahead-of-eid>
- Mandra. (2024). The Ministry of Communication and Information Receives Hundreds of Thousands of Online Fraud Complaints. Taken from Radio Republik Indonesia: <https://rri.co.id/nasional/951055/kemenkominfo-terimaratusan-ribu-aduan-penipuan-online>
- Monetary Authority of Singapore. (2024). Combatting Scams. Retrieved from Monetary Authority of Singapore: <https://www.mas.gov.sg/regulation/combating-scams>

- OJK. (2022). Task Force Profile. Retrieved from the Financial Services Authority: <https://ojk.go.id/waspadainvestasi/id/tentang/Pages/Profil-Satgas.aspx>
- Financial Services Authority. (2026, January 22). The Indonesia Anti-Scam Centre managed to return Rp161 billion in funds from scam victims. <https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/IASC-Berhasil-Kembalikan-Rp161-Miliar-Dana-Masyarakat-Korban-Scam.aspx>
- Peter Mahmud Marzuki (2013), *Legal Research* (Revised edition), Jakarta: Kencana Prenada Media Group, p.133
- Rachel, F. (2025). OJK Requires Banks to Join the Anti-Scam Center Task Force, What Is the Reason. Retrieved from Tempo.Co: <https://www.tempo.co/ekonomi/ojk-wajibkan-bank-bank-gabung-dalam-satgas-antiscam-center-apa-alasannya--31302>
- Riana, P. (2024). *Anti-Fraud Guide: Consumer Strategies to Avoid Fraud and Fraudulent Business Practices*. Surabaya. CV. Garuda Mas Sejahtera.
- Soerjono Soekanto and Sri Mamuji (2013). *Normative Law Research: A Brief Review*. Jakarta: Raja Grafindo Persada, p. 13
- Singapore Police Force. (2025). Annual Scams and Cybercrime Brief 2024. <https://www.police.gov.sg/-/media/Spf/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2024/Annual-Scams-and-Cybercrime-Brief-2024.ashx>
- Syadid, J. A. (2025). Comparison of Cybercrime Laws Between Indonesia and Singapore. *Journal of Law and Citizenship*, Volumes 10, 11.
- Tech for Good Institute. (2025). Building Resilience against Scams and Fraud: Spotlight on Indonesia. Taken from Tech for Good Institute <https://techforgoodinstitute.org/blog/event-highlights/building-resilience-againstscams-and-fraud-spotlight-on-indonesia/>
- United Nation Office on Drugs and Crime. (2024). Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Retrieved from United Nations Office on Drugs and Crime: [https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC\\_Convergence\\_Report\\_2024.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf)
- Vienna, V. (2025). Singapore needs a multi-layered strategy to fight fraud. Taken from Banking & Finance: <https://asianbankingandfinance.net/indonesian/exclusive/singapura-membutuhkanstrategi-berlapis-untuk-melawan-penipuan>
- Wallinda, M. F. (2025). Fraud Victims in Singapore Increase Every Year. Taken from Radio Republik Indonesia: <https://www.rri.co.id/internasional/1354277/korbanpenipuan-di-singapura-meningkat-tiap-tahun>
- Wibowo, D. E. (2024). The Comparison of Indonesian and American Customer Protection Laws: What and How?. *SASI*, 30(4).
- Wicaksono, S. R. (2020). *Fraud and Scam in the Digital Era: Concept and Development*. CV. Thousand Stars
- Yap, A. (2024). Anti-Scam Centre of the Singapore Police Force: Fighting Scams is a Community Effort. Retrieved from Singapore Police Force:

<https://www.gasa.org/post/anti-scam-centre-of-the-singapore-police-force-fightingscams-is-a-community-effort>

Yuyut, P. (2024). The Dynamics of Consumer Legal Protection in the Digital Era: Legal Analysis of E-Commerce Practices and Consumer Data Protection in Indonesia. *Journal of Legal Interpretation*, Volume 5 Number 1, 907