



EXAMINING THE LEGAL FRAMEWORK GOVERNING SMS FRAUD SCHEMES IN SEMARANG CITY

Praditya Arcy Pratama

Faculty of Law, Universitas PGRI Semarang
pradityaarcypratama@upgris.ac.id

Lintang Enggartiasto

Faculty of Engineering, Universitas PGRI Semarang
lintangenggartiasto@upgris.ac.id

Rudiadi

Faculty of Engineering, Universitas PGRI Semarang
rudiadi.r@uin-suska.ac.id

Martomo

Faculty of Engineering, Universitas PGRI Semarang
martomo@upgris.ac.id

Abstract: Public legal awareness and understanding of how to report fraud through Short Message Service (SMS) remain limited despite the Electronic Information and Transactions Law (ITE Law). This empirical legal study examines SMS fraud in Semarang City. The findings identify weak law enforcement, limited public literacy, and rapid technological change as barriers to prevention and enforcement. Respondents also reported inadequate public outreach about SMS fraud risks. The study highlights the need for an integrated response combining legal education, stronger enforcement, and greater public awareness. Cooperation among government, law enforcement agencies, telecommunications providers, and the public is essential to improve protection against SMS fraud.

Keywords: Short Message Service (SMS), ITE Law, Fraud, Law Enforcement

INTRODUCTION

Developments in the field of information and communication technology have brought significant changes to the way humans interact, including in aspects of everyday communication. One communication application that is now very popular throughout the world is the mobile phone. With the number of active users reaching billions across various parts of the world, the use of mobile phones has evolved into a primary tool for individuals to send messages, make calls, and share information quickly and efficiently. Mobile phones not only function as communication tools, but have also evolved into

multifunctional devices that support various user needs. With the availability of various applications, mobile phones enable users to connect with others, both directly and indirectly, through various platforms. This demonstrates how important the role of technology is in facilitating social interaction in this modern era.

In this context, it can be seen that the use of mobile phones has become an integral part of people's daily lives. These devices provide convenience in communication, both for personal and professional purposes. In addition, mobile phones also contribute to increased productivity, as users can access information and communicate with colleagues or friends at almost the

same time, without being hindered by distance. The development of social media in Indonesia has had a major impact on various aspects of life, including communication, business, and entertainment. However, behind its benefits, social media has also become fertile ground for the emergence of fraudulent criminal acts through various schemes, such as online buying and selling scams, fictitious investments, and the dissemination of malicious links through social media. There are even scams carried out through Short Message Service (SMS). The prevalence of these scams has caused concern among the public because they often result in significant material losses (Harapansyah et al., 2024; Fazry, 2023).

Based on information obtained from Cyber Patrol, it was recorded that the public had filed a total of 14,496 police reports. These reports covered various types of scams, including Online Scams, Investment Scams, Lottery and Prize Scams, Employment and Labor Scams, Technical Support Scams, Romance Scams, Credit Card Scams, as well as Online Shopping Scams. This significant number of reports shows that the public is becoming increasingly aware of the various types of scams that are widespread online. This also indicates the need for further action from the authorities to address and prevent scams that harm many people (Patroli Siber, 2025).

One common form of cybercrime or crime in cyberspace is phishing. Phishing is a criminal act in cyberspace that aims to steal individuals' information and personal data by exploiting various communication channels, such as

email, telephone, text messages, or links that appear legitimate. Phishing perpetrators usually pretend to be a trusted organization or party, making victims feel safe providing the requested information. The term "scam" itself refers to an unconventional act of fraud, derived from the words "fishing" or "digging". In this context, scammers try to "persuade" individuals to provide sensitive data that can then be misused for their own benefit. Sensitive data that is often targeted includes passwords, credit card information, email addresses, and one-time passwords (OTPs). The data successfully stolen by these scammers can be used for various criminal acts, such as theft, identity theft, and extortion (Hadiyati & Stathany, 2021; Oktaviana & Rinaldi, 2025; Universitas Bakrie, 2025; Frensh, 2021).

To address this issue, the government enacted Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which has undergone several amendments, the first being Law Number 19 of 2016 and the second being Number 1 of 2024 concerning the Electronic Information and Transactions Law. The ITE Law plays an important role as a legal basis for prosecuting perpetrators of fraud through social media or fraud based on electronic transactions, while also providing protection for internet users in Indonesia. Based on the provisions stipulated in Law Number 1 of 2024 concerning Electronic Information and Transactions, particularly Article 28 paragraph 1, it is clearly regulated that any individual who intentionally distributes and/or transmits Electronic Information and/or Electronic

Documents containing false or misleading information, which may result in material losses for consumers in the context of Electronic Transactions, will be subject to criminal sanctions. These sanctions consist of imprisonment for a maximum duration of six years and/or a fine of up to IDR 1,000,000,000 (one billion rupiah) (Sitanggang et al., 2023; Akbar et al., 2024).

The role of the ITE Law in regulating criminal acts of fraud through short message services in Semarang City demonstrates how important legal regulations are in addressing the very rapid advancement of information technology. In today's digital era, the use of short message services has become one of the most common methods of communication. However, behind this convenience, various fraudulent schemes have emerged that exploit technology to harm the public. Fraud through SMS, for example, is often carried out by sending messages pretending to be a certain party, such as claiming to be a distant relative living away from home, then a bank or even a government institution, requesting personal information or asking for a money transfer. This makes the public vulnerable targets of such criminal acts. With the existence of clear provisions in the ITE Law, law enforcement officials have a legal basis for taking action against perpetrators of digital crimes. The ITE Law not only regulates electronic information and transactions, but also provides clear sanctions for perpetrators of cybercrime. For example, based on Article 28 paragraph (1) of the ITE Law, it is stated that anyone who intentionally

and without authorization disseminates information intended to deceive another person may be subject to criminal sanctions. This provision provides legal certainty for law enforcement officials in handling cases of fraud through SMS. In practice, law enforcement authorities in Semarang City have taken various measures, such as educating the public about common fraud schemes, as well as apprehending identified fraud perpetrators (Putri & Kurniawan, 2021).

Regulations concerning the enforcement of the law against perpetrators of fraud through SMS need to be strengthened. Law enforcement must utilize modern technology to detect and prevent fraud before it occurs. The use of monitoring systems capable of identifying suspicious patterns in SMS transmissions could be an effective first step. In addition, increasing the capacity of human resources within law enforcement agencies is very important so that they are better prepared to face increasingly complex crimes. Training and education for law enforcement officers regarding the latest developments in information technology and the various existing fraud schemes are crucial. The role of the ITE Law in regulating criminal acts of fraud through SMS is vital in the context of the rapid development of information technology. With clear regulations in place, law enforcement officers have a basis for taking action against digital criminals and protecting the public (Direktorat Jenderal Ekosistem Digital, 2026).

RESEARCH QUESTIONS

This study examines SMS fraud and public legal awareness in Semarang City.

RESEARCH METHOD

This study uses an empirical legal research method to examine how law operates in society. It focuses on the application of legal rules in practice, individuals' experiences of legal processes, and social phenomena that may not be fully captured in written legal sources (Widiarty, 2019).

The empirical approach considers both legal norms and their application in everyday life. It examines public behavior and the social conditions affecting understanding and enforcement of the law. This approach is used here to identify practical challenges in addressing SMS fraud in Semarang City and to inform responses to those challenges.

RESULTS AND DISCUSSION

The phenomenon of fraud occurring through Short Message Service (SMS) in Semarang City shows that this method is still widely used and causes concern among the public. Based on the results of the interviews conducted, all respondents (100%) admitted that they had received SMS messages containing fraud in various forms, such as prize offers, requests to transfer money, and claims of being close relatives. This reality shows that SMS remains a highly effective means for cybercriminals, given its direct nature, low cost, and ease of access for the general public. The high number of fraudulent messages received also reflects weaknesses in the monitoring system as well as the limited

preventive measures taken by telecommunications service providers and law enforcement authorities. Furthermore, this study also reveals that the public's response to fraudulent SMS messages generally tends to be passive. Most respondents chose to ignore these messages (77.8%), while only a small number took the initiative to delete or report them (22.2%). This situation indicates that public legal awareness and understanding of the procedures for reporting electronic-based criminal offenses are still relatively low. Although the Electronic Information and Transactions Law (UU ITE) and other related regulations have stipulated criminal sanctions for perpetrators of online fraud, including fraud committed through SMS, the implementation of these laws has not yet been fully perceived as effective by the public. This is particularly evident in the aspects of consumer protection and the prosecution of perpetrators.

It is clear that there is a need to increase public awareness and understanding of the dangers of fraud through SMS as well as the existing reporting mechanisms. Educational and outreach efforts regarding the UU ITE and consumer rights must be increased so that the public becomes more vigilant and proactive in addressing this issue. In addition, collaboration between telecommunications service providers and law enforcement authorities is also very important to create a better monitoring system and more effective preventive measures. Only through a comprehensive approach can we reduce the incidence of fraud through SMS and improve the security and comfort of the public in communicating.

Table 1. Public Respondents' Experiences and Perceptions of SMS Fraud in Semarang City

#	Question	Response	Percent
1	Have you received fraudulent SMS messages?	Yes/Often	100%
2	Response to fraudulent SMS messages	Ignore	77.8%
		Ignore and delete/report	22.2%
3	Main targets of SMS fraud	Everyone	83.3%
		Older adults	16.7%
4	Know how to report SMS fraud?	No	77.8%
		Yes	22.2%
5	Effect on sense of security	Severely disrupted	72.2%
		Unaffected	27.8%
6	Is government outreach sufficient?	No/Insufficient	94.4%
		Sufficient	5.6%
7	Have you or a relative been a victim?	Yes (self/relative)	55.6%
		Never/Do not know	44.4%
8	Why is SMS fraud difficult to combat?	Weak law enforcement	38.9%
		Low public literacy	27.8%
		Technological developments	22.2%
		Other	11.1%
9	Role of law enforcement in Semarang	Poor	44.4%
		Fairly good	33.3%
		No role	22.3%
10	Mobile service provider	Telkomsel	61.1%
		Indosat	22.2%
		Three	16.7%
11	Received SMS messages impersonating a relative or neighbor?	Yes	55.6%
		No	44.4%

From the perspective of the general public, the majority of respondents believe that SMS scams can affect all segments of society, with a percentage reaching 83.3%. Nevertheless, there is also a view among a small portion of respondents, namely 16.7%, who stated that vulnerable groups such as the elderly are more at risk of becoming victims. This indicates that SMS scam modus operandi are widespread and know no boundaries, so preventive efforts are needed that include legal education as

well as improving digital literacy for all elements of society. It is interesting to note that more than half of the respondents, namely 55.6%, revealed that they or their family members had been direct victims of this scam. This indicates that the impact of such crimes is very real and is not merely a hypothetical threat.

On the other hand, there are several factors that hinder efforts to eradicate this crime. The majority of respondents identified weak law enforcement, at 38.9%, as one of the

main causes that makes it difficult to deal with perpetrators of this crime. In addition, the low level of public literacy regarding scam methods, recorded at 27.8%, as well as the rapid development of communication technology, at 22.2%, also contribute to this problem. This shows that although legal regulations such as the ITE Law are already in place, their effectiveness depends greatly on the consistency and commitment of law enforcement officials as well as the public's ability to understand and anticipate various new scam methods.

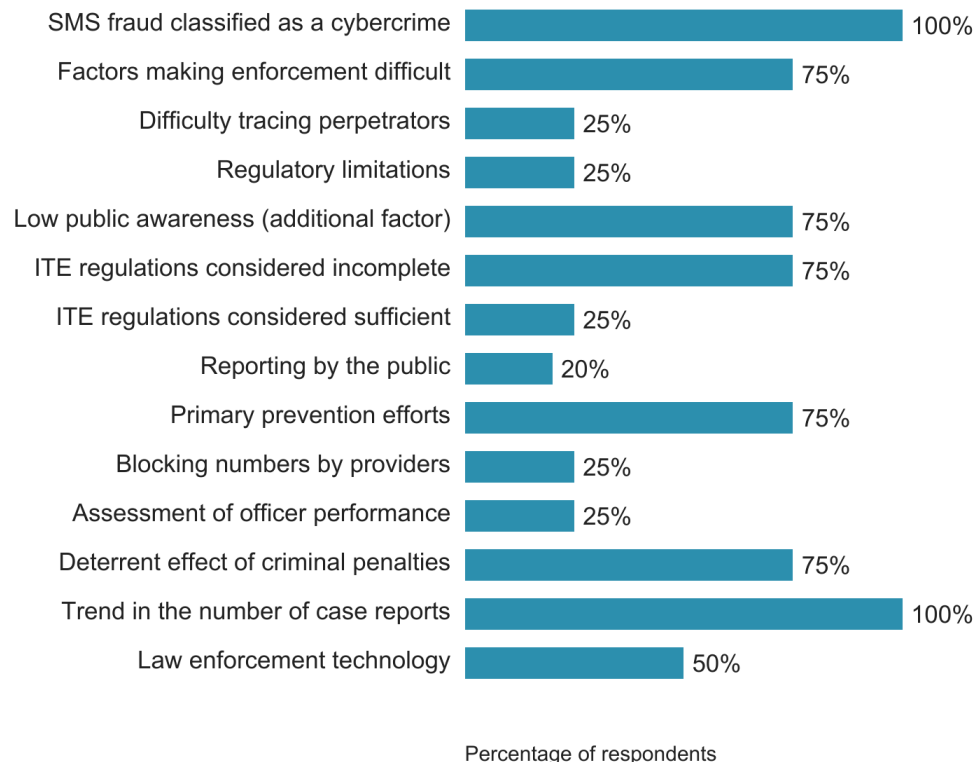
Regarding the role of law enforcement officials in Semarang City, respondents' assessments indicate that their performance is not yet optimal. As many as 44.4% of respondents assessed that the role of law enforcement officials was poor, while another 33.3% assessed their performance as fairly good, and 22.3% even stated that there was no role at all. This situation reflects a significant gap between the regulations that have

been established and their implementation in the field. In addition, the public outreach conducted by the government regarding the dangers of SMS scams is also considered inadequate. As many as 94.4% of respondents stated that the existing outreach was still insufficient. This emphasizes the importance of a collaborative approach between the government, law enforcement officials, telecommunications service providers, and the public to create a more effective and comprehensive protection system.

To address the challenge of SMS scams, a more integrated strategy involving various parties is needed. Comprehensive education, stricter law enforcement, and increased public awareness of existing scam methods must be the main focus. Only through synergistic joint efforts can we build a society that is safer and better protected from the threat of SMS scams.

Survey Responses from Law Enforcement Practitioners, Including Lawyers, Police Officers, and Mediators

Survey Results from Law Enforcement Practitioners



Overall consensus (100%): SMS fraud is considered a cybercrime, and the number of reports regarding these cases shows a significant increase. The majority of respondents (75%) believe that there are several main factors causing this problem. First, the difficulty of tracking down perpetrators is a major challenge. In addition, they also consider that the existing regulations in the Electronic Information and Transactions Law (UU ITE) are still incomplete for effectively addressing this issue. Cooperation between law enforcement agencies and telecommunications service providers is considered not to be working well, so the primary prevention effort is through firm law enforcement. Although the performance of law enforcement

agencies is considered fairly good, the existing criminal penalties are deemed insufficient to deter perpetrators.

In the divided view (50%-50%), there are differences of opinion regarding case reporting by the public, with some believing that such reporting rarely occurs, while others feel that reporting is frequently carried out. In addition, there are also differing views regarding which parties play the greatest role in addressing this issue, between law enforcement agencies and the government and service providers.

In the varied assessment (25%-50%-25%), there is variation in the assessment of the technology used by law enforcement agencies. Some respondents consider the existing technology still inadequate, while

others feel it is sufficient, and there are also those who consider the technology to be highly adequate for handling these SMS fraud cases. With a deep understanding of this issue, it is important for all parties to work together in seeking effective solutions to address SMS fraud. Firm law enforcement, improvements in regulations, as well as increased cooperation between law enforcement agencies and service providers are crucial steps to reduce the number of fraud cases and provide a sense of security to the public.

CONCLUSION

The phenomenon of SMS scams in Semarang City remains very common and causes anxiety among the public. All respondents in this study acknowledged that they had received scam-related SMS messages, with the majority tending to react passively, namely by simply ignoring the messages. The level of legal awareness and public understanding of how to report SMS scams is quite low. Although there are laws such as the ITE Law that regulate sanctions for perpetrators of online crimes, the effectiveness of implementing these laws remains questionable. Most respondents believe that SMS scams can happen to anyone, especially more vulnerable groups such as the elderly. More than half of the respondents admitted that they had been victims of scams. Several factors that make it difficult to eradicate these scams include weak law enforcement, low levels of public literacy, and very rapid technological developments. Assessments of the performance of law enforcement officers showed unsatisfactory results, with many respondents feeling that public

outreach regarding the risks of SMS scams remains very limited.

To address this issue, a more integrated strategy is needed, including legal education, stricter law enforcement, and increased public awareness. Cooperation between the government, law enforcement agencies, telecommunications service providers, and the public is essential to building an effective protection system. With a comprehensive approach, it is hoped that the number of SMS scams can be reduced and that people will feel safer.

REFERENCES

- [1] Akbar, M. A., Kamal, M., & Badaru, B. (2024). Efektivitas Peran Kepolisian Terhadap Penegakan Hukum Tindak Pidana Penipuan Online Di Dunia Maya. *Journal of Lex Philosophy (JLP)*, 5(2), 877–893. <https://pasca-umi.ac.id/index.php/jlp/article/view/1867>
- [2] Universitas Bakrie. "Kenalan Dengan 5 Jenis-Jenis Phising Yang Patut Diwaspadai!," 2025. <https://bakrie.ac.id/articles/599-kenalan-dengan-5-jenis-jenis-phising-yang-patut-diwaspadai.html>.

- [3] Fazry, Muhammad. "Sosialisasi Undang-Undang ITE Di Era Digital: Membangun Kesadaran Dan Tanggung Jawab Di Kalangan Pelajar SMK 3 Tidore." *BARAKATI: Journal of Community Service* 02, no. 1 (2023): 1–6. <http://ejournal.sangadjimediapublishing.id/index.php/barakati/article/view/54/85%0Ahttps://ejournal.sangadjimediapublishing.id/index.php/barakati/article/download/54/84>.
- [4] Frensh, Wenggedes. "Penanggulangan Tindak Pidana Siber Dengan Menggunakan Teori Jendela Pecah." *Doktrina: Journal of Law* 4, no. 2 (2021): 159–69. <https://doi.org/10.31289/doktrina.v4i2.5793>.
- [5] Hadiyati, Nur, and Hayllen Stathany. "Analisis Undang-Undang Ite Berdasarkan Asas Pembentukan Peraturan Perundang-Undangan Di Indonesia." *Mizan: Jurnal Ilmu Hukum* 10, no. 2 (2021): 146. <https://doi.org/10.32503/mizan.v10i2.1657>.
- [6] Harapansyah, M, S Rahman, and B Badaru. "The Effectiveness of Law Enforcement for Criminal Fraud via WhatsApp in the Legal Area of the Pasangkayu Police." *International Journal on Advanced Science, Education, and Religion (IJoASER)* 7, no. 1 (2024): 77–93.
- [7] Oktaviana, Helma, and Kasmanto Rinaldi. "Modus Operandi Phisher Dalam Kejahatan Phishing (Studi Kasus Ditreskrimsus Polda Riau)." *Journal of Knowledge and Collaboration* 2, no. 5 (2025): 655–58.
- [8] Patroli Siber. "Jumlah Laporan Polisi Yang Dibuat Masyarakat," 2025. <https://patrolisiber.id/statistic/>.
- [9] Putri, Hanuring Ayu Ardhani, and Itok Dwi Kurniawan. "Penanggulangan Tindak Pidana Penipuan Menggunakan Media Handphone (Sms)." *Jurnal Pendidikan Politik, Hukum, Dan Kewarganegaraan* 11, no. 2 (2021): 33–39.
- [10] Sitanggang, Adelina, Bertania Permata Sari, Eirene Dahlia Sidabutar, Halimah, Mira Cahya, and Ramsul Yandi Nababan. "Penegakan Undang-Undang ITE Terhadap Kasus Judi Online." *Mediation: Journal of Law* 2, no. 4 (2023): 16–22. <https://pusdikrapublishing.com/index.php/jhkm/article/view/1620>.
- [11] Widiarty, Wiwik Sri. *Buku Ajar Metode Penelitian Hukum. RISTANSI: Riset Akuntansi*, 2019. <http://repository.uki.ac.id/14688/1/BukuAjarMetodePenelitianHukum.pdf>.
- [12] Direktorat Jenderal Ekosistem Digital, 2026, Waspada Smishing: Ancaman Penipuan Lewat SMS yang Perlu Diwaspadai, <https://djed.komdigi.go.id/news/waspada-smishing-ancaman-penipuan-lewat-sms-yang-perlu-diwaspadai>