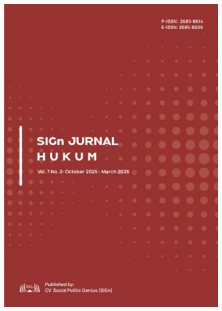


# SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614
https://jurnal.penerbitsign.com/index.php/sjh/article/view/v7n2-29

Vol. 7 No. 2: October 2025 - March 2026 Published Online: January 24, 2026


Article Title

## The Effectiveness of Law Enforcement on Cybercrime: A Case Study of Online Fraud in South Sulawesi

Author(s)


**Zulfan Akbar Syahfallah***
*Universitas Muslim Indonesia, Indonesia || syahfallahzulfanakbar@gmail.com*
**Corresponding Author*

**Askari Razak**
*Universitas Muslim Indonesia, Indonesia || askari.razak@umi.ac.id*

**Salle Salle**
*Universitas Muslim Indonesia, Indonesia || salle.salle@umi.ac.id*



How to cite:

Syahfallah, Z. A., Razak, A., & Salle, S. (2026). The Effectiveness of Law Enforcement on Cybercrime: A Case Study of Online Fraud in South Sulawesi. *SIGn Jurnal Hukum, 7*(2), 1116-1130. https://doi.org/10.37276/sjh.v7i2.557

**ABSTRACT**

*The escalation of cyber fraud offenses within the South Sulawesi Regional Police's jurisdiction poses serious challenges for law enforcement authorities, particularly given the limitations of conventional regulatory instruments that fail to address the characteristics of digital crime. This research aims to conduct an in-depth analysis of law enforcement disparity triggered by the normative gap between the application of Article 378 of Law Number 1 of 1946 and Law Number 11 of 2008 and its amendments, evaluate structural and cultural obstacles distorting investigation effectiveness, and project a systemic solution through the transition to Law Number 1 of 2023. Employing a socio-legal research method with a qualitative approach, this study integrates doctrinal analysis with empirical data obtained through in-depth interviews with investigators, judges, and victims. The results reveal crucial facts regarding regulatory disharmony, where law enforcement officials experience inertia in exercising their authority to cut off digital access due to unprepared forensic infrastructure at the regional level and low public legal literacy. This phenomenon creates a paradox of blunt law enforcement and perpetuates disparities in court verdicts. In conclusion, this study asserts that partial reform is no longer adequate to address the complexity of cybercrime. The study's implications include concrete steps, such as formulating standard operating procedures aligned with Article 493 of Law Number 1 of 2023, forensic laboratory decentralization, and adopting internet access rights revocation sanctions as a futuristic sentencing strategy that guarantees legal certainty and restorative justice.*

*Keywords:* *Criminal Law Transition; Cybercrime; Fraud; Law Enforcement Disparity; Normative Gap.*

## INTRODUCTION

Accelerated digital transformation has positioned information technology as a primary necessity in the modern human life ecosystem, fundamentally altering the patterns of social and economic interaction. High dependence on digital platforms, particularly in electronic transactions and financial services, not only increases efficiency but also creates new vulnerabilities to cybercrime. This phenomenon is confirmed by the study of Nur and Panggabean (2021), which showed that the massive adoption of digital payment methods among the younger generation is directly proportional to increased security risks. In a broader context, Ekawati et al. (2025) asserted that the banking and e-commerce sectors have now become the epicenter of cyberattacks, where phishing and social engineering are the most dominant modus operandi for exploiting user negligence.

Indonesia, particularly the South Sulawesi region, is facing an alarming escalation in cyber fraud cases, even as internet penetration is not matched by adequate digital literacy. Data from the Ministry of Communication and Digital (Komdigi) showed that by mid-2025, more than 1.2 million reports of digital fraud had been recorded through the national public complaint system, with financial losses totaling trillions of rupiah (Sakina, 2025). Specifically at the local level, empirical research by Adrianto et al. (2024) and Akbar et al. (2024) indicated that the police in South Sulawesi were overwhelmed by the surge in cyber fraud reports, ranging from fictitious buying and selling to fraudulent investments. This high crime rate creates a security paradox

within society, where the digital space that should be a productive medium has metamorphosed into a fertile ground for predatory criminal actors.

The fundamental issue in combating this crime lies in the normative gap between conventional legal instruments and the characteristics of cybercrime, which are borderless and anonymous. Law enforcement officials were often forced to use Article 378 of Law Number 1 of 1946 to entrap cyber fraud perpetrators (Rauf et al., 2024). However, the construction of this article requires elements of a "series of lies" and physical meetings, which are difficult to prove in the context of electronic transactions. On the other hand, the existence of Law Number 11 of 2008 and its amendments was often not utilized optimally as *lex specialis* due to interpretative confusion among investigators (Triananda et al., 2024). Consequently, regulatory disharmony occurred, causing legal uncertainty in case handling.

In addition to substantive legal challenges, the effectiveness of law enforcement in South Sulawesi is also distorted by complex structural and cultural obstacles. The study by Sihombing et al. (2024) highlighted that technological innovation at the Resort Police level is often hindered by limited digital forensic facilities and human resource competence. This is exacerbated by a permissive and pragmatic legal culture within the community. This was observed in cases of online rotating savings schemes and fraudulent investments, where victims were often tempted by instant profits without verifying their legality (Alamsyah et al., 2023; Rahmawati, 2024). Nuraksari et al. (2024) added that in Umrah travel fraud cases, victims' limited legal awareness to report incidents contributed to the expansion of the dark figure of crime untouched by the judicial process.

The urgency of this research peaks at the momentum of the national criminal law transition, where Indonesia has moved from the regime of Law Number 1 of 1946 to Law Number 1 of 2023. This situation demands a critical evaluation of law enforcement officials' readiness to adopt the new sentencing paradigm, including measures to protect consumers from fraudulent practices, as analyzed by Zuvarcan et al. (2025) in the context of service fraud. The absence of a clear roadmap during this transition period has the potential to perpetuate verdict disparities and failure in victim protection, thus necessitating a comprehensive study to bridge the gap between *das sollen* (legal expectation) and *das sein* (current law enforcement reality).

Based on these problems, this research aims to conduct an in-depth analysis of three crucial aspects. First, to analyze law enforcement disparities arising from the normative gap between the reliance on Article 378 of Law Number 1 of 1946 and the *lex specialis* instruments in Law Number 11 of 2008 and its amendments. Second, to evaluate structural and cultural obstacles that distort the effectiveness of cyber investigation authority within the jurisdiction of the South Sulawesi Regional Police,

particularly regarding the execution of cutting off access to digital assets. Third, to project the juridical implications of the transition to Law Number 1 of 2023 as a systemic solution to reduce legal uncertainty and verdict disparities in the future.

## METHOD

This study employs socio-legal research that combines a doctrinal analysis of positive legal norms with an empirical study on the operation of law in society (Qamar & Rezah, 2020). This approach was chosen to dissect the complexity of cyber fraud issues stemming not only from statutory texts but also from the dynamic interactions between law enforcement officials, victims, and local community culture. The main focus is directed at analyzing the disparity between *das sollen* (what ought to be according to the new law) and *das sein* (what actually occurred in the field) in 2025, taking specific locations within the jurisdiction of the South Sulawesi Regional Police, including the Makassar Police Resort and Gowa Police Resort, which represent the centers of highest digital activity in the region.

Data sources in this study are classified into two complementary main categories (Sampara & Husen, 2016). Primary data were collected directly in the field through in-depth interviews with purposively selected key informants, including cybercrime unit investigators, criminal law academics, district court judges, and cyber fraud victims. The selection of informants was based on criteria of competence, case handling experience, and direct relevance to the object of study. Meanwhile, secondary data include primary legal materials, such as Law Number 1 of 1946, Law Number 11 of 2008 and its amendments, and Law Number 1 of 2023, as well as secondary legal materials in the form of literature, scientific journals, and annual reports of relevant agencies related to the cybercrime discourse.

Data collection techniques were carried out through source and method triangulation to ensure information validity (Miles et al., 2014). Interviews were conducted using semi-structured guidelines to explore officials' subjective perspectives on the technical constraints and regulatory conflicts they faced. Parallel to this, documentation studies of court decisions and police reports were conducted to map patterns of disparity in case handling. The collected data were then reduced, systematically presented, and verified for validity before proceeding to the analysis stage, ensuring no interpretative bias in the reading of the legal facts.

Data analysis was conducted in a qualitative-prescriptive manner through three systematic stages aligned with the research objectives (Irwansyah, 2020). The first stage is the normative gap analysis, in which the author confronts the practice of officials using conventional articles with the availability of *lex specialis* instruments under Law Number 11 of 2008 and its amendments. The second stage is the evaluation

of structural and cultural obstacles, dissecting the correlation between limited digital forensic facilities and low public legal literacy and their impact on law enforcement effectiveness. The third stage is the futuristic projection, examining the potential of articles in Law Number 1 of 2023 as a systemic solution to resolve the current legal deadlock. This entire series of analyses culminates in drawing deductive conclusions, namely deriving general propositions from specific field findings to formulate concrete policy recommendations.

## RESULTS AND DISCUSSION

### A. Normative Gap: Application Conflict between Article 378 of Law Number 1 of 1946 and Instruments of Law Number 11 of 2008

Law enforcement practices regarding cyber fraud crimes within the South Sulawesi Regional Police's jurisdiction reflect a sharp dissonance between available legal instruments and the norms actually applied by officials. Although Law Number 11 of 2008 has undergone a second amendment through Law Number 1 of 2024, which reinforces cyber offenses, field findings in 2025 showed that investigators still had a strong tendency to use Article 378 of Law Number 1 of 1946 as the primary basis for charging suspects. This dependence on conventional articles is not merely a matter of technical preference but rather an indication of a substantial lack of understanding of the specific characteristics of digital crimes, which are borderless and non-physical (Rauf et al., 2024).

This normative gap stems from the construction of Article 378 of Law Number 1 of 1946, which requires rigid material elements, such as "using a false name," "false capacity," "deceit," or "a series of lies" to induce others to hand over goods. In the context of conventional crime, proving these elements requires a physical meeting or direct interaction that can be visibly verified. However, when applied to cyber modi operandi such as phishing or e-commerce algorithm manipulation, the element of "a series of lies" becomes extremely difficult to prove because the interaction occurs through electronic system intermediaries that are often anonymous. This difficulty was confirmed by RK, an Investigator at the South Sulawesi Regional Police, who revealed the operational dilemma at the investigation level:

> *"Law Number 11 of 2008 and its amendments indeed contain provisions regarding unlawful acts in cyberspace, but the formulation of electronic fraud offenses has not been regulated in detail. Consequently, law enforcement officials often resort to catchall articles or fraud provisions in Article 378 of Law Number 1 of 1946, which have not fully accommodated the characteristics of cybercrime."*

This statement validates the analysis of Triananda et al. (2024), who found that the effectiveness of cybercrime prevention is often hindered by officials' confusion in selecting the appropriate legal instrument. In fact, the *lex specialis* instrument has juridically provided for this through Article 28 section (1) of Law Number 1 of 2024, which emphasizes the element of spreading false news resulting in "consumer loss." This article was designed to reduce the burden of proving the complex element of "deceit" under Law Number 1 of 1946 by shifting the focus to the material loss suffered by consumers in electronic transactions. However, the lack of uniform technical implementation guidelines led investigators to hesitate in applying this specialist article, prompting them to revert to Article 378 of Law Number 1 of 1946, which is considered more familiar but is now obsolete.

The condition of regulatory disharmony is exacerbated by the complexity of proof in cases involving cross-jurisdictional digital financial transactions. The study by Opit and Frans (2025) regarding fraud evidence in the capital market provided a relevant analogy, where crimes involving electronic data manipulation require a standard of proof far more sophisticated than mere conventional eyewitnesses. In cyber fraud cases in South Sulawesi, there was often overlap in interpretation over whether a case was purely criminal fraud or a civil breach of contract, especially in online buying and selling, where goods were not shipped or did not match the order. This doubt created a legal loophole that perpetrators exploited to escape criminal charges under the pretext of a regular trade dispute. RK, an Investigator at the South Sulawesi Regional Police, asserted that this uncertainty directly impacted law enforcement consistency:

> *"In practice, confusion often occurs regarding whether a case falls into the realm of conventional fraud (Law Number 1 of 1946) or electronic-based fraud (Law Number 11 of 2008 and its amendments). This leads to inconsistency in court decisions."*

Such inconsistency aligns with the findings of Alamsyah et al. (2023) in their analysis of fraudulent investment cases, where the application of layered charges often confused judges and resulted in verdicts disproportionate to victims' losses. When officials hesitate to determine the offense qualification, the principle of legal certainty becomes the main victim. Ruslan (2022), in his study on international trade fraud, also highlighted that without a shared understanding of the operational definition of fraud in the digital realm, law enforcement efforts would be only reactive and partial, unable to reach the roots of organized crime syndicates.

The failure to fully shift to the *lex specialis* paradigm, specifically Law Number 11 of 2008 and its amendments, also contributed to the lack of systematic

preventive measures. Rafique and Venugopal (2021) emphasized that fraud risk mitigation should be built on regulations capable of early detection of transaction anomalies, rather than merely punishing perpetrators after losses occur. In South Sulawesi, reliance on Law Number 1 of 1946, which is oriented toward retribution, often neglects the recovery of victims' losses. Adrianto et al. (2024) noted that the majority of cyber fraud victims in this region did not receive refunds because the investigation focused on proving the perpetrator's element of "lies" rather than pursuing asset recovery.

The role of the police as the vanguard of law enforcement becomes crucial yet vulnerable in this normative transition situation. Akbar et al. (2024) underscored that the effectiveness of the police role relies heavily on the ability to adapt to new legal instruments. AC, as an Academic/Criminal Law Expert, offered sharp criticism of the inertia of the legal system, which is still confined by the old paradigm:

> *"The issue of electronic fraud is not sufficiently handled by old regulations. Law Number 1 of 1946 still uses classical concepts, while crime modes are already very modern. There is Law Number 11 of 2008 and its amendments, but the articles are open to multiple interpretations. So, substantially, our law is indeed not ready."*

The expert's statement confirms that the current normative gap is not merely a technical juridical issue but a paradigmatic one. The dependence on Article 378 of Law Number 1 of 1946 is a symptom of the legal system's unpreparedness to respond to the evolution of digital crime. This conflict of norm application ultimately creates a bottleneck in the criminal justice system, where officials' energy is drained debating articles while victims continue to fall without adequate protection. This situation of substantive uncertainty serves as the entry point to more complex problems at the operational level, namely institutional structural unpreparedness and community cultural resistance, which will be discussed in the next section.

## B. Law Enforcement Disparity: The Paradox of Cyber Authority and Cultural Obstacles

The regulatory disharmony outlined previously is merely the tip of the iceberg regarding the complexity of cyber law enforcement issues in South Sulawesi. Beneath the surface lies a sharp disparity between broad juridical authority and technical execution capacity in the field. Normatively, Article 43 section (5) letter l of Law Number 1 of 2024 has granted highly progressive authority to investigators to order the cutting off of access to social media accounts, bank accounts, and digital assets related to criminal acts. This authority was essentially designed to

bypass banking bureaucracy, which has long been a primary obstacle in securing proceeds of crime. However, the operational reality at the South Sulawesi Regional Police presents a paradox: this sophisticated "weapon" becomes blunt in the hands of officials unsupported by adequate forensic infrastructure.

This technological gap is confirmed by the study by Sihombing et al. (2024), which highlighted that the effectiveness of investigations in the digital era relies heavily on technological innovation at the territorial unit level. Without the support of responsive digital forensic laboratories at the Police Resort level, tracking volatile digital footprints in real time becomes impossible. This condition is exacerbated by uneven human resource (HR) competence, as revealed by MN, an Investigator at the Gowa Police Resort:

> *"Not all law enforcement officials possess competence in the field of information technology. In fact, handling electronic fraud cases requires a deep understanding of the cyber world, digital disguise techniques, and even digital forensics."*

The investigator's statement validates the analysis of Akbar et al. (2024) regarding the crucial role of the police, which is often hindered by internal factors. When cybercriminals employ advanced encryption technologies or cross-border servers to conceal their identities, local officials are instead grappling with manual procedures. MK, an Investigator at the Cybercrime Unit of the South Sulawesi Regional Police, added a complaint regarding the slowness of the evidentiary process due to facility centralization:

> *"We actually have a cyber unit in the region, but facilities are limited. For digital forensic analysis, we sometimes have to send [evidence] to the center, which takes a long time. Whereas digital footprints disappear very quickly."*

This delay is fatal in the context of cybercrime proof. Oktana et al. (2023) emphasized that the validity of electronic evidence depends heavily on the speed of data acquisition. When digital evidence is secured too late due to laboratory bureaucracy, data integrity is vulnerable to challenge in court, ultimately weakening the public prosecutor's position. This structural paradox creates a situation in which the law appears present through fierce statutes but is paralyzed when confronted with technical realities on the ground.

In addition to structural obstacles, law enforcement effectiveness is also distorted by cultural factors rooted in the community's behavior as potential victims. Recent data from the Ministry of Communication and Digital showed that Indonesia's e-commerce ecosystem faces high security risks due to low user digital literacy (Sakina, 2025). The study by Ekawati et al. (2025) on phishing

in the banking sector found that cyberattacks now exploit human psychological factors (human error) more than technical system loopholes. In South Sulawesi, this phenomenon is clearly visible in the rampant fraud cases involving fraudulent investments and online rotating savings schemes, in which victims voluntarily handed over money due to being tempted by irrational instant profits (Rahmawati, 2024).

This pragmatic and permissive culture becomes a dominant criminogenic factor. Nuraksari et al. (2024), in their study on Umrah travel fraud, found that perpetrators often manipulated religious sentiments to dull victims' critical faculties. Similarly, Gadjong (2023) and A'Raaf et al. (2024) noted that in cases of personal shopper services or car sales via social media, victims often ignored basic verification procedures such as checking accounts or seller identities for the sake of low prices. JK, a Judge at the Makassar District Court, highlighted this cultural phenomenon in trial sessions:

> *"I often see cyber fraud victims attracted by the lure of getting rich quickly or cheap goods. This has become a cultural norm, easily tempting. So, actually, there is an element of negligence on the part of the community as well. If the public were more careful, the number of cases could decrease."*

This weakness in legal culture is further aggravated by widespread technology adoption among the younger generation, which is not balanced by risk awareness, as analyzed by Nur and Panggabean (2021). TJ, a victim of cyber fraud, reflected the despair resulting from a combination of ignorance and slow official response:

> *"I reported to the police, but they said the perpetrator was hard to track because they used a fake account. I also didn't know what evidence I had to prepare. Finally, I felt it was useless and chose to remain silent."*

The frustration of victims like TJ creates a cycle of distrust toward the criminal justice system. When the law fails to provide preventive protection through literacy and retributive justice through swift action, the community tends to become apathetic. The accumulation of this regulatory disharmony, structural technical paralysis, and cultural vulnerability demands a radical systemic solution. Partial improvements are no longer adequate; a transformation of the sentencing paradigm is required to bridge this gap through more futuristic and certain legal instruments, which will be elaborated in the transition projection toward Law Number 1 of 2023.

## C. Criminal Transition Projection: Law Number 1 of 2023 and Digital Sanction Innovation as a Systemic Solution

The law enforcement deadlock caused by regulatory disharmony and structural paralysis demands a radical transformation of the sentencing paradigm. Partial improvements through mere addition of tools or socialization will not suffice to unravel the tangled threads of legal disparity that have taken root. Therefore, the momentum for enacting Law Number 1 of 2023 in 2026 must be positioned as a starting point for systemic reform. The urgency of this transition is evident from legal practitioners' complaints about the uncertainty surrounding sentencing parameters under the current legal regime. JK, a Judge at the Makassar District Court, expressed his anxiety regarding verdict disparities that erode the public's sense of justice:

> *"In trials, the most frequent debate concerns electronic evidence. For instance, WhatsApp screenshots require additional corroboration; they cannot stand alone. Consequently, many cases have weak evidentiary support. Furthermore, there is a disparity in verdicts; some are sentenced heavily, others lightly, even though the modus operandi is the same. This makes the public doubt justice."*

The complained disparity is rooted in the excessive flexibility within Law Number 1 of 1946, which lacks standard sentencing parameters based on economic loss values. In the future, Law Number 1 of 2023 offers a concrete solution through Article 79, which establishes a fine system based on categories (Category I to VIII), and Article 494, which specifically classifies "minor fraud" for losses below a certain limit. This mechanism will reduce judicial subjectivity and provide more measurable legal certainty. Hutahaean and Indarti (2020), in their study on crime eradication strategies within the Police force, emphasized that institutional reform must begin with regulatory standardization that limits discretion prone to deviation. With the rigid parameters set out in Law Number 1 of 2023, law enforcement officials in South Sulawesi have clear guidelines for processing small-scale but massive cases that have frequently been ignored.

In addition to providing sentencing certainty, Law Number 1 of 2023 also closes the normative loophole often exploited by perpetrators of online buying and selling fraud. TJ, a victim of cyber fraud, reflected on how the current law failed to reach the modus operandi of rogue sellers:

> *"I was once deceived in online shopping; the seller vanished after I transferred the money. When I reported it to the police, they said it was difficult to track because the account was under another person's name. I was also confused about what evidence to provide. In the end, there has been no result until now. It feels useless to report."*

TJ's complaint represents the failure of Article 378 of Law Number 1 of 1946, which is difficult to apply to breach of contract cases turning into fraud. As a solution, Article 493 of Law Number 1 of 2023 explicitly criminalizes sellers who hand over goods different from what was agreed upon or provide false information regarding the nature and condition of the goods. This article adopts progressive consumer protection principles. Zuvarcan et al. (2025), in their analysis of the legal framework for healthcare fraud, asserted that the shift in modern criminal law is toward protecting consumers from fraudulent practices that result in economic loss, rather than merely on the element of physical deceit. Applying this logic in handling cybercrime will facilitate investigators in entrapping perpetrators without being burdened by proving the complicated element of a "series of lies."

However, regulatory reform alone is insufficient if the imposed sanctions fail to provide a deterrent effect for cybercrime perpetrators who are often recidivists. Amirullah and Sodikin (2026) introduced the concept of "Digital Sentencing Innovation" as an additional sanction: the revocation of internet access rights for cyber offenders. This concept is highly relevant to Indonesia's sentencing guidelines, as physical imprisonment often fails to prevent perpetrators from committing cyber fraud again using mobile devices from behind bars. This digital right revocation sanction aligns with the spirit of Law Number 1 of 2023, which accommodates supervision penalties and community service, providing sentencing alternatives that are more effective in breaking the chain of cybercrime.

In facing organized cyber fraud syndicates, proof strategies must also evolve. Sukadana et al. (2018) highlighted the importance of using justice collaborator testimony to dismantle complex criminal structures. Given that many cyber fraud syndicates in South Sulawesi operate in clandestine cells, the application of a leniency program scheme for perpetrators who cooperate will become a vital instrument under the new criminal procedure regime in Law Number 20 of 2025. This must be supported by strengthening alternative dispute resolution mechanisms for minor cases. Kharisma and Ar (2022) suggested optimizing Online Dispute Resolution (ODR) as a rapid settlement path for consumer disputes in fintech and e-commerce, thereby reducing the burden of case accumulation in police and courts and allowing officials to focus on serious cybercrimes.

Overall, the transition to Law Number 1 of 2023 is not merely a change in legal documents, but a systemic transformation that addresses the failure of the old paradigm. The integration of norm certainty in Articles 493 and 494 of Law Number 1 of 2023, digital sanction innovations, and modern proof strategies offers a comprehensive roadmap to overcome current law enforcement disparities. The success of this projection implementation will depend heavily on law enforcement

officials in South Sulawesi's readiness to shed conventional mindsets and adapt to futuristic legal instruments oriented towards victim loss recovery and justice certainty.

## CONCLUSIONS AND SUGGESTIONS

This study concludes that the law enforcement disparity regarding cyber fraud crimes within the jurisdiction of the South Sulawesi Regional Police is fundamentally rooted in intertwined regulatory disharmony and structural paradoxes. Normatively, there is a sharp gap between investigation practices that still rely on the conventional paradigm of Article 378 of Law Number 1 of 1946 and the *lex specialis* instruments in Law Number 11 of 2008 and its amendments, which have not been fully utilized. The reliance on this obsolete article hinders the prosecution of anonymous, physically borderless digital crimes, thereby creating a loophole for perpetrators' impunity. On the other hand, the effectiveness of progressive authority, such as the Law's mandate to cut off access to digital assets, is distorted by the unpreparedness of forensic infrastructure at the regional level and the resistance of a legal culture within a society with low digital literacy and pragmatic tendencies. Consequently, law enforcement operates only partially and fails to provide a significant deterrent effect or to achieve maximal victim recovery.

To overcome this deadlock, the transition toward the enactment of Law Number 1 of 2023 in 2026 is projected to be a systemic solution capable of reducing legal uncertainty and verdict disparities that have long been the subject of complaint. The construction of Article 493 of the Law, which specifically criminalizes seller fraud, provides a more precise juridical foundation than general fraud cases under Article 492 of the Law. Meanwhile, the classification of minor fraud under Article 494 of the Law provides judges with measurable sentencing parameters. This regulatory transformation not only closes the legal loopholes exploited by perpetrators but also shifts the sentencing orientation from mere retribution to equitable consumer protection, while simultaneously addressing the challenges posed by future legal needs demanding certainty and speed.

As an implication of these findings, it is recommended that the South Sulawesi Regional Police immediately formulate standard operating procedures for handling cybercrime that integrate the instruments of Law Number 11 of 2008 and its amendments with the transition preparation for Law Number 1 of 2023, accompanied by the decentralization of digital forensic laboratory facilities down to the resort level to accelerate the evidentiary process. Furthermore, it is necessary to strengthen criminal policy at the national level by adopting sanction innovations, such as revoking internet access for cybercrime recidivists, to provide more effective deterrence than

conventional imprisonment. The synergy between futuristic legal substance renewal, responsive institutional structure strengthening, and cultural intervention through massive public education becomes an absolute prerequisite for realizing a secure and legally certain digital ecosystem in South Sulawesi.

## REFERENCES

A'Raaf, F. A., Rahman, S., & Badaru, B. (2024). Perlindungan Hukum bagi Konsumen Korban Penipuan Jual Beli Mobil Melalui Aplikasi Facebook. *Journal of Lex Theory (JLT)*, *5*(1), 253-268. Retrieved from https://pasca-umi.ac.id/index.php/jlt/article/view/1678

Adrianto, A., Thalib, H., & Ilyas, M. (2024). Penegakan Hukum Terhadap Tindak Pidana Penipuan Online. *Journal of Lex Philosophy (JLP)*, *5*(2), 1445-1457. Retrieved from https://pasca-umi.ac.id/index.php/jlp/article/view/1946

Akbar, M. A., Kamal, M., & Badaru, B. (2024). Efektivitas Peran Kepolisan Terhadap Penegakan Hukum Tindak Pidana Penipuan Online di Dunia Maya. *Journal of Lex Philosophy (JLP)*, *5*(2), 877-893. Retrieved from https://pasca-umi.ac.id/index.php/jlp/article/view/1867

Alamsyah, F. R., Cameron, C., Ridwan, P., Yustisia, M. T., Romadhon, M. R. R., & Yusuf, N. T. (2023). Problems in the Application of Law in the Indra Kenz Fraudulent Investment Case. *The Digest: Journal of Jurisprudence and Legisprudence*, *4*(1), 1-20. https://doi.org/10.15294/digest.v4i1.67847

Amirullah, S., & Sodikin, S. (2026). The Principle of Legality vs. Digital Sentencing Innovation: The Dialectics of Revocation of Internet Access Rights as a Criminal Penalty in Cybercrime Cases. *SIGn Jurnal Hukum*, *7*(2), 1078-1096. https://doi.org/10.37276/sjh.v7i2.553

Ekawati, D., Herdiana, D., & Haryanti, A. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. *SIGn Jurnal Hukum*, *7*(1), 133-151. https://doi.org/10.37276/sjh.v7i1.422

Gadjong, A. A. (2023). The Agreement of Personal Shopping Service through E-Commerce Platforms: A Case Study of Consumer Protection. *SIGn Jurnal Hukum*, *4*(2), 388-401. https://doi.org/10.37276/sjh.v4i2.230

Hutahaean, A., & Indarti, E. (2020). Strategi Pemberantasan Korupsi oleh Kepolisian Negara Republik Indonesia (Polri). *Masalah-Masalah Hukum*, *49*(3), 314-323. https://doi.org/10.14710/mmh.49.3.2020.314-323

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Kharisma, D. B., & Ar, N. T. E. (2022). Online Dispute Resolution as an Alternative Model for Dispute Settlement in the Financial Technology Sector. *Pandecta Research Law Journal*, *17*(1), 137-145. https://doi.org/10.15294/pandecta.v17i1.25267

Law of the Republic of Indonesia Number 1 of 1946 on the Penal Code Regulations. https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/814

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/138

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1683

Law of the Republic of Indonesia Number 1 of 2023 on the Penal Code (State Gazette of the Republic of Indonesia of 2023 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6842). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1818

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1842

Law of the Republic of Indonesia Number 20 of 2025 on the Criminal Procedure Code (State Gazette of the Republic of Indonesia of 2025 Number 188, Supplement to the State Gazette of the Republic of Indonesia Number 7149). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/2011

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (Third Edition). Sage. https://books.google.co.id/books?id=p0wXBAAAQBAJ

Nur, T., & Panggabean, R. R. (2021). Factors Influencing the Adoption of Mobile Payment Method among Generation Z: The Extended UTAUT Approach. *Journal of Accounting Research Organization and Economics*, *4*(1), 14-28. https://doi.org/10.24815/jaroe.v4i1.19644

Nuraksari, Y., Thalib, H., & Salle, S. (2024). Efektivitas Penyidikan Tindak Pidana Penipuan Travel Umrah. *Journal of Lex Theory (JLT)*, *5*(2), 745-762. Retrieved from https://pasca-umi.ac.id/index.php/jlt/article/view/1852

Oktana, R., Akub, S., & Maskun, M. (2023). Social Media in the Process of Evidence of Electronic Information and Transaction Crimes. *SIGn Jurnal Hukum*, *4*(2), 320-331. https://doi.org/10.37276/sjh.v4i2.252

Opit, S. E., & Frans, M. P. (2025). Proving Securities Trading Fraud in Capital Market Crimes. *SIGn Jurnal Hukum*, *7*(1), 54-69. https://doi.org/10.37276/sjh.v7i1.413

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn). https://books.google.co.id/books?id=TAQHEAAAQBAJ

Rafique, R. B., & Venugopal, V. (2021). Preventive Measures to Mitigate the Risk of Fraud in Letters of Credit Transactions in Malaysia. *UUM Journal of Legal Studies*, *12*(1), 27-49. https://doi.org/10.32890/uumjls.12.1.2021.7882

Rahmawati, N. D. (2024). Law Enforcement against Online Arisan Fraud Perpetrators Who Conduct Fictitious Arisan Auctions (Case Study of Sukoharjo Police Station Cases). *Serunai*, *2*(2), 107-114. https://doi.org/10.63019/serunai.v2i2.54

Rauf, A., Rahman, S., & Razak, A. (2024). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Melalui Media Elektronik. *Journal of Lex Philosophy (JLP)*, *5*(1), 77-93. Retrieved from https://pasca-umi.ac.id/index.php/jlp/article/view/1624

Ruslan, Z. (2022). Letter of Credit: Uniform Custom Practice dan Fraud dalam Perdagangan Internasional. *Equity: Jurnal Ekonomi*, *10*(2), 117-126. https://doi.org/10.33019/equity.v10i2.118

Sakina, P. (2025, October 15). *Komdigi: Keamanan Ekosistem E-commerce Jadi Tanggung Jawab Bersama*. Antara. Retrieved November 22, 2025, from https://www.antaranews.com/berita/5176273/komdigi-keamanan-ekosistem-e-commerce-jadi-tanggung-jawab-bersama

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Sihombing, R. P., Kusno, K., & Siregar, A. A. (2024). Investigative Effectiveness in the Digital Era: A Case Study of Technological Innovation at the Rokan Hilir Police Resort. *SIGn Jurnal Hukum*, *6*(2), 52-67. https://doi.org/10.37276/sjh.v6i2.368

Sukadana, I. M., Amiruddin, A., & Parman, L. (2018). Alat Bukti Keterangan Saksi Mahkota dalam Perkara Pidana Pencurian. *Law Reform*, *14*(2), 262-274. https://doi.org/10.14710/lr.v14i2.20873

Triananda, R. K., Razak, A., & Mappaselleng, N. F. (2024). Efektivitas Pencegahan dan Penanggulangan Tindak Pidana Penipuan Jual Beli Online. *Journal of Lex Philosophy (JLP)*, *5*(2), 471-486. Retrieved from https://pasca-umi.ac.id/index.php/jlp/article/view/1808

Zuvarcan, D. A., Yuspin, W., & Budiono, A. (2025). Qualitative Study of Fraud in Health Services and Legal Framework in Indonesia: A Literature Review. *Diponegoro Law Review*, *10*(1), 42-53. https://doi.org/10.14710/dilrev.10.1.2025.42-53