Jurnal Pembaharuan Hukum
Volume 12, Number 3, December 2025
E-ISSN : 2355 – 0481 (Print)
ISSN : 2580 – 3085 (Online)

LEGAL EFFECTIVENESS OF ARTICLE 492 OF THE NEW CRIMINAL CODE IN ADDRESSING DIGITAL FRAUD AGAINST MSMES IN BANJARMASIN

Dadang Abdullah
Universitas Lambung Mangkurat, Banjarmasin, Indonesia
dadang.abdullah@ulm.ac.id

Abdul Halim Barkatullah
Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Tavinayati
Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Andi Asari
Universitas Teknologi MARA Shah Alam, Selangor, Malaysia

ARTICLE INFO

Keywords:
Criminal Code; Criminal Law; Digital Fraud; Digital literacy; Legal protection.

ABSTRACT

The digital era has transformed the business landscape of traditional market traders and MSMEs in various regions, presenting new opportunities while also increasing the risk of online fraud. This study aims to analyse the effectiveness of Article 492 of the New Criminal Code in tackling digital fraud and protecting vulnerable small business actors. The method used is qualitative with a descriptive-analytical approach, combining normative legal studies and empirical data from interviews with market traders, MSME associations, cybercrime apparatus, and representatives of e-commerce platforms. This study analyzes primary legal sources, such as Article 492 of the New Criminal Code. The results of the study reveal a significant knowledge gap, with 75% of respondents being unaware of Article 492's existence. The four main factors of vulnerability identified are low digital literacy, limited access to legal information, weak coordination with law enforcement officials, and dominance of large e-commerce platforms. To overcome this, this study offers a three-pillar coordination model, namely law enforcement, improving legal and digital literacy, and an application-based integrated reporting system. These findings confirm that effective digital criminal law requires not only regulation, but also cross-sector synergy and stronger public legal awareness.

A. INTRODUCTION

The digital transformation has fundamentally reshaped the business landscape of traditional market traders and Micro, Small, And Medium

Enterprises (MSMEs) in Banjarmasin. The rapid development of information technology, particularly through e-commerce platforms and electronic payment systems, has created new opportunities for business actors to expand market reach, enhance operational efficiency, and strengthen competitiveness in an increasingly dynamic economic environment.[1] Digitalization enables traditional market traders who were previously dependent on face-to-face transactions to access consumers beyond geographical boundaries.[2] The Indonesian government has actively responded to this transformation by accelerating MSME digitalization through various policy initiatives, including programs intensified by the Ministry of Cooperatives and SMEs since 2023. These initiatives focus on basic digital training, the adoption of digital platforms, and the strengthening of human resource capacity to ensure that micro-business actors can adapt to the evolving digital ecosystem. Such efforts are supported by national digital literacy campaigns aimed at improving public awareness and competence in the safe and productive use of digital technologies.[3]

Despite these significant opportunities, digital transformation also introduces new challenges and risks, particularly the increasing prevalence of cybercrime targeting MSMEs and traditional market traders. Low levels of digital literacy among these business actors make them especially vulnerable to modern forms of digital fraud, including online store identity forgery, transaction manipulation, and electronic payment scams.[4] Previous studies indicate that digital literacy plays a crucial role in improving business performance by enhancing market orientation and operational efficiency (Yanto et al., 2022).[5] However, digital literacy gaps remain a persistent issue

[1] Abu Muna Almaududi Ausat, "In-depth study of the strategic interaction between electronic commerce, innovation, and attainment of competitive advantage in the context of SMEs," *International Journal of Analysis and Applications* 23 (2025): 78.

[2] Abdul Wahid, "Measuring the Effectiveness of the New Criminal Code in Answering Contemporary Criminal Law Challenges," *Lex Journal: Kajian Hukum Dan Keadilan* 9, no. 1 (2025): 49.

[3] Muhammad Ardiansyah Satria Dwi Putra, and Ifahda Pratama Hapsari, "Implikasi Sanksi Pemidanaan di Dalam KUHP Baru Terhadap Delik Penipuan Transaksi Secara Online," *UNES Law Review* 7, no. 3 (2025): 1066. See too, Cahya Wulandari, Sugianto Sugianto, Anggyi Trisnawan Putra, Zidney Ilma Fazaada Emha, and Muhamad Sayuti Hassan, "Literacy, Compliance, and Digital Legal Awareness: The Role of JDIH UNNES in Disseminating Legal Information," *Indonesian Journal of Advocacy and Legal Services* 7, no. 1 (2025): 238.

[4] Sahlan Efendi, Hendra Sukarman, Iwan Setiawan, and Muhammad Amin Effendy, "Analisis tindak pidana penipuan pasal 378 undang-undang nomor 1 tahun 1946 dibandingkan dengan pasal 492 undang-undang nomor 1 tahun 2023," *Pustaka Galuh Justisi* 3, no. 2 (2025): 182.

[5] Dina Elisa Putri, Elly Sudarti, and Elizabeth Siregar, "Tindak Pidana Penipuan Melalui Aplikasi Digital (Gagasan Pemikiran Pertanggungjawaban Oleh Bank)," *PAMPAS: Journal of Criminal Law* 5, no. 1 (2024): 76. See too, Heri Yanto, Niswah Baroroh, Ain Hajawiyah, and Nurhazrina Mat Rahim, "The Roles of entrepreneurial skills, financial literacy, and digital literacy in maintaining MSMEs during the COVID-19 Pandemic," *Asian Economic and Financial Review* 12, no. 7 (2022): 504.

among MSMEs in Banjarmasin. This vulnerability is exacerbated by weak coordination among cyber law enforcement agencies, digital platform providers, and merchant associations, resulting in slow reporting and investigation processes. Although the Indonesian government has enacted a new Criminal Code that explicitly regulates cyber fraud through Article 492, its implementation at the operational level remains limited and inconsistent, leaving legal loopholes that can be exploited by fraud perpetrators.[6] Furthermore, existing administrative sanctions are considered insufficient to create a deterrent effect, allowing cyber fraud activities to continue with relatively low risk for offenders.[7]

In this context, the present study is both important and urgent. The lack of empirical data regarding the frequency, patterns, and economic impacts of digital fraud experienced by MSMEs and traditional market traders in Banjarmasin hampers the formulation of effective and evidence-based policies. This research aims to identify the factors contributing to the high incidence of digital fraud cases and assess the effectiveness of Article 492 within the context of Banjarmasin MSMEs, utilising a cross-sectoral synergy approach. Filling regulatory gaps and increasing digital literacy are considered essential because consumer trust is a key prerequisite for digital economy growth. The objectives of the study are: (1) to identify the regulatory and operational gaps of Article 492; (2) formulate a coordination model between cyber apparatus, digital platforms, and market traders; and (3) to test the synergy can significantly reduce the rate of digital fraud in Banjarmasin.

B. RESEARCH METHODS

This study uses a qualitative approach with a descriptive-analytical method to examine and explain legal issues related to digital fraud, as well as to assess the effectiveness of implementing Article 492 of the New Criminal Code among traditional market traders and MSMEs in Banjarmasin. By integrating normative and empirical legal research, it provides a holistic view of legal issues by combining theoretical analysis with practical insights. This approach can increase the relevance and impact of legal studies, making them more responsive to real-world challenges and societal needs. Despite the challenges of incorporating these methodologies, the benefits of a comprehensive understanding of the law justify the effort.[8] The goal is to build

[6] C. Nugroho, A. Wulandari, D. Maulana, N. Rina, and A. F. Kalaloi, "Digital communication and literacy for MSME empowerment: Evidence from a rural digital village in Indonesia," *International Journal of Innovative Research and Scientific Studies* 8, no. 3 (2025): 4526.

[7] Mey Richa Madya Lestari, *Methods of Teaching Arabic*, (Omsk: Economic of Region, 2009), 23.

[8] Tenzin Wangmo, Veerle Provoost, and E. Mihailov, "The vagueness of integrating the empirical and the normative: Researchers' views on doing empirical bioethics," *Journal of Bioethical Inquiry* 21, no. 2 (2024): 299.

a deep understanding of the gap between regulation and practice, as well as to seek real data-driven solutions.

The data source consists of secondary data and primary data. Secondary data includes the New Criminal Code (Law Number 1 of 2023), derivative regulations, guidelines from the Ministry of Cooperatives and SMEs, and the latest scientific literature analysed using document analysis techniques. Primary data were obtained through in-depth interviews with 12 respondents, including market traders, representatives of MSME associations, Cyber Crime Task Force officers, and representatives of e-commerce platforms, as well as case studies on digital fraud crimes that have been handled.

The analysis of legal problems is carried out systematically in three stages. First, identify the regulatory gap between the legal text of Article 492 of the New Criminal Code and the reality of implementation among business actors. Second, a critical analysis of empirical findings uses a thematic analysis approach to uncover the factors that affect the vulnerability of MSMEs to fraud. Third, the integration of the findings from both approaches will inform policy recommendations and synergy models between institutions for effective digital law prevention and enforcement. This approach ensures the transparency, validity, and reproducibility of the research.

C. DISCUSSION

1. Identification of Regulatory Gaps in Article 492 of the New Criminal Code

Article 492 of the New Criminal Code (Law Number 1 of 2023) was essentially formulated as a legal instrument to address various forms of digital fraud that are increasing in tandem with the advancement of information technology. This norm is expected to become a legal umbrella, protecting the community, especially small business actors, traditional market traders, and MSMEs who are increasingly involved in the digital trade ecosystem. However, the findings in the field show that this normative function has not been reflected in practice. Instead of being a protective instrument, this regulation remains "hidden" from the legal consciousness of the community, which should be the primary beneficiaries.[9]

The ineffectiveness of this implementation is evident from the empirical fact that the majority of market traders not only do not understand the content of the article, but have never even heard of the existence of the rule at all.[10] For some traders, their understanding of digital fraud is still limited to the

[9] Siti Sri Wulandari, Mohd Lizam Bin Mohd Diah, and Andi Asari, "Digital proficiency and entrepreneurial mindset for sme success through market savvy and tech literacy," *Aptisi Transactions on Technopreneurship (ATT)* 7, no. 1 (2025): 28.

[10] Saeed Akhtar, and Siba Borah, Prasad, *Regulatory Frameworks and Digital Compliance in Green Marketing*, (Hershey: IGI Global, 2025), 23.

notion that the only way to resolve it is through a police report. This view suggests that criminal norms intended to provide legal certainty are actually disconnected from social reality. In the framework of legal awareness theory, this condition illustrates that awareness of the law has not reached the stage of knowledge of the law, let alone attitude and behaviour toward the law.[11]

Furthermore, the results of interviews with 12 respondents provide a worrying quantitative picture. A total of 9 people (75%) were unfamiliar with Article 492, while 3 people (25%) had only heard of it through online news without understanding its substance. None of the respondents had a complete understanding of the content or procedures of its implementation. Academically, this indicates a fairly sharp knowledge gap between national-level regulators and the community of business actors at the grassroots level. This knowledge gap is not only a problem of information that is not conveyed, but also a structural problem in the process of legal socialisation that does not reach the community groups that should be protected.[12]

This condition has profound implications for the effectiveness of criminal law in the context of digital economy protection. A regulation, no matter how comprehensive normatively, will lose its binding force if it is not accompanied by enforcement and legal literacy.[13] This means that the existence of Article 492 of the New Criminal Code will only stop as a legal text (law in the book) without ever really functioning as a law in action. When the majority of legal subjects do not understand the existence of norms, regulations lose their practical legitimacy and are unable to cause deterrent or preventive protection effects.

Progressive legal theory advocates the priority of justice over rigid adherence to legal mandates. This involves ethical and political decision-making that responds to deliberation and public engagement.[14] In Indonesia, for example, a progressive legal approach suggests that unjust laws can be ignored in favour of upholding justice by integrating moral and ethical roles into legal practice.[15] Without a bridging mechanism in the form of socialisation, education, and cross-institutional coordination, legal norms have the potential

[11] Ermek Abdrasulov, Akmaral Saktaganova, Indira Saktaganova, Sayash Zhenissov, and Zhassulan Toleuov, "Legal awareness and its significance when determining the nature of a person's legal behaviour," *International Journal of Electronic Security and Digital Forensics* 15, no. 6 (2023): 578.

[12] Sora Park, J. Ramon Gil-Garcia, Theresa A. Pardo, Megan Sutherland, and Andrew Roepe, "Cross-boundary information sharing in regulatory contexts: The case of financial markets," *Public Money & Management* 39, no. 5 (2019): 348.

[13] Di Fan, Andy CL Yeung, Daphne W. Yiu, and Chris KY Lo, "Safety regulation enforcement and production safety: The role of penalties and voluntary safety management systems," *International Journal of Production Economics* 248 (2022): 108481.

[14] Colin Grey, "Bureaucracy without alienation," (2020): 126.

[15] Lisma, "Progressive law functions in realizing justice in Indonesia," *Syariah: Jurnal Hukum dan Pemikiran* 19, no. 1 (2019): 3.

only to become a "dead letter" that is never effective. Thus, the findings of this study affirm the urgency of state intervention in the form of more massive information dissemination, legal guidance that directly touches traditional market communities, and mechanisms to strengthen digital legal literacy among MSMEs.[16]

In summary, the ignorance of the majority of market traders towards Article 492 cannot be seen solely as an individual weakness, but rather as a reflection of the weak policy design of the socialisation of the criminal law. The information gap that arises is not only a knowledge gap, but also has the potential to increase people's economic vulnerability because they are not aware of the existence of legal instruments that can be used to protect themselves from digital fraud practices. This is what makes the knowledge gap in the context of Article 492 of the New Criminal Code not only a cognitive problem, but also a structural and institutional problem that needs to be addressed immediately.

Table 1. Level of Market Traders' Knowledge about Article 492 of the New Criminal Code (n = 12 respondents)

Respondent Knowledge Categories	Respondent Knowledge Categories	Percentage	Information
Not knowing at all	9	75%	Never heard of Article 492; Consider that cases can only be handled by the police
Have heard, but do not understand	3	25%	Information from online media without technical understanding
Knowing and understanding in its entirety	0	0%	None of the respondents understood the content and procedures of Article 492

Source: Field Interviews, 2025; processed by the author.

Table 1 findings learly show that there is a real knowledge gap between regulators and business actors at the grassroots level. The knowledge gap is not only informational, namely the lack of knowledge of market traders about the substance of Article 492 of the New Criminal Code, but also structural due to the absence of an effective legal communication mechanism. In other words, even though regulations are already present as written norms, they fail

[16] Martha Hasanah Rustam, Hamler Hamler, Tat Marlina, Duwi Handoko, and Rahmad Alamsyah, "Peran dan tanggung jawab konsumen untuk mencegah praktik penipuan dalam transaksi online dari perspektif hukum perlindungan konsumen," *Riau Law Journal* 7, no. 1 (2023): 13.

to reach legal subjects who should derive direct protection from their existence.

The obstacles to implementation do not only lie on the community side, but also in the technical aspects faced by law enforcement officials. The Banjarmasin Police Cyber Satreskrim Unit, for example, acknowledged that, in the process of proof, there are still significant challenges. Article 492 can indeed be used as a formal legal basis, but the evidentiary process is often stalled because the provisions in the New Criminal Code are not fully aligned with the evidentiary mechanism in the Information and Electronic Transactions Law (*Undang Undang Informasi dan Transaksi Elektronik*/ITE Law). Regulatory synchronisation and the implementation of cutting-edge technology solutions are essential for the effective use of digital evidence in fraud cases. This ensures that electronic evidence is reliable, secure, and admissible in court, thereby improving the integrity of the overall judicial process.[17]

The unclear position of the electronic evidence has implications for the weak position of the victim in the legal process. Law enforcement officials often face a dilemma between acknowledging digital evidence as legitimate evidence or rejecting it because it does not conform to conventional criminal evidentiary standards.[18] As a result, many cases of digital fraud end up stopping at the reporting stage without ever reaching the prosecution process. This shows that the New Criminal Code, especially Article 492, is still experiencing what in the legal literature is referred to as regulatory lag.[19] This term describes a phenomenon where written law lags behind social and technological dynamics, rendering it unable to address the practical needs of society adequately.

In a broader framework, this regulatory lag not only reduces the effectiveness of Article 492 but also erodes public trust in the criminal law as a means of protection. For market traders and MSMEs, the experience of being rejected because digital evidence is considered weak will create the perception that the criminal law is not present to protect them. If this condition continues, then the existence of norms has the potential to lose its social legitimacy. Therefore, serious efforts are needed to draft derivative rules that integrate the New Criminal Code with the ITE Law, especially in the aspects of validation and standardisation of electronic evidence. It is this integration that will

[17] Fu-Ching Tsai, "The application of blockchain of custody in criminal investigation process," *Procedia Computer Science* 192 (2021): 2780.

[18] Kanika Pandit, and Renu Mahajan, "Advancing Digital Forensics: Harnessing Blockchain for Evidence Authentication," In *2024 Second International Conference on Advanced Computing & Communication Technologies (ICACCTech)*, (IEEE, 2024), 219.

[19] Handar Subhandi Bakhtiar, Amir Ilyas, Abdul Kholiq, and Handina Sulastrina Bakhtiar, "The utilisation of scientific crime investigation methods and forensic evidence in the criminal investigation process in Indonesia," *Egyptian Journal of Forensic Sciences* 15, no. 1 (2025): 39.

determine whether Article 492 can truly function as an effective instrument in reducing the number of digital fraud cases in society.

The results of the in-depth interview provide a reasonably comprehensive picture of the structural vulnerability of MSMEs in Banjarmasin in dealing with digital fraud crimes. The thematic analysis reveals four interrelated factors that reinforce each other, creating conditions that render market traders and MSME actors legally and economically vulnerable.

One of the most prominent factors emerging from the findings is the low level of digital literacy, which opens substantial space for cybercrime to occur. Many merchants still use simple devices without adequate account protection, do not understand two-factor authentication procedures, and are not wary of phishing or social engineering scams. As a result, they tend to be easily fooled into making transactions, providing personal data, and even handing over access to digital accounts to irresponsible parties. This condition suggests that digital transformation does not necessarily coincide with the improvement of digital skills in small merchant groups.

This vulnerability is further compounded by limited access to legal information, which significantly exacerbates the risks faced by MSMEs. Most respondents have never received socialisation related to Article 492 of the New Criminal Code or other digital consumer protection regulations. The absence of this information leaves them unaware of their legal rights and the procedures they can take when they become victims of fraud. Thus, this low legal knowledge not only has implications for the lack of prevention, but also has an impact on their inability to fight for rights when they are already victims.

At the institutional level, weak coordination between traders and law enforcement officials reveals a serious structural gap in fraud handling mechanisms. Some respondents admitted that the reports submitted often did not receive follow-up because the evidence submitted was considered invalid. This causes a negative perception of the apparatus and weakens traders' confidence to involve criminal law as a means of settlement. In other words, even though regulations are available, the absence of effective coordination renders the law ineffective in the eyes of the victim.

Beyond state institutions, the dominance of large e-commerce platforms places MSMEs in a subordinate position within digital dispute resolution processes. The platform's internal policies often determine the outcome of disputes more than the applicable legal norms. For small traders, this reduces the sense of security as their bargaining positions are almost non-existent. They must be subject to terms and conditions unilaterally created by the platform, while access to formal legal instruments is severely limited. This situation reflects the asymmetric power relationship between small businesses

and large tech companies, which ultimately increases the vulnerability of market traders to digital fraud practices.

If these four factors are viewed integratively, it is clear that the vulnerability of MSMEs is not just an individual problem, but a combination of literacy, legal, institutional, and digital market structures that are unequal.[20] Low digital literacy makes it easy for traders to become victims, limited access to legal information prevents them from seeking protection, weak coordination with the authorities reduces trust in the legal system, while the dominance of large platforms further closes the substantive justice space. As such, these vulnerabilities are systemic and require a multidimensional approach that focuses not only on the criminal law aspect but also on capacity building, the provision of access to legal information, and the improvement of digital platform governance.

Table 2. Vulnerability Factors of MSMEs to Digital Fraud (n = 12 respondents)

Vulnerability Factors	Number of Respondents	Persentase	Field Findings
Low digital literacy	8	67%	The majority of traders do not understand account security and payment verification.
Limited access to legal information	10	83%	There has never been any socialisation of Article 492 of the New Criminal Code at the trader level.
Weak coordination with the apparatus	7	58%	The report was rejected because evidence of digital conversation was deemed invalid.
Dominance of large e-commerce platforms	6	50%	Disputes are determined by the platform's internal policies, not formal legal norms.

Source: Field Interviews, 2025; processed by the author.

Table 2 illustrates that MSMEs in Banjarmasin face multiple, overlapping vulnerability factors that increase their exposure to digital fraud. Limited access to legal information emerges as the most dominant issue, reported by

[20] Nur Khusniyah Indrawati, Sri Muljaningsih, Himmiyatul Amanah Jiwa Juwita, A. Muhamad Jazuli, Nuraini Desty Nurmasari, and Mochammad Fahlevi, "The mediator role of risk tolerance and risk perception in the relationship between financial literacy and financing decision," *Cogent Business & Management* 12, no. 1 (2025): 2468. See too, Ni Kadek Marlita Erdiana Putri, Kadek Januarsa Adi Sudharma, AA Ayu Ngurah Sri Rahayu Gorda, and AA Ayu Intan Puspadewi, "Kebijakan Yuridis dan Implementasi Perlindungan Konsumen Bitcoin dalam Menghadapi Ancaman Penipuan Online di Indonesia," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3, no. 4 (2025): 3919.

83% of respondents, reflecting the absence of socialisation regarding Article 492 of the New Criminal Code at the trader level. Low digital literacy also constitutes a major vulnerability, affecting 67% of respondents who lack basic understanding of account security and payment verification mechanisms. In addition, weak coordination with law enforcement authorities was experienced by 58% of respondents, particularly in cases where fraud reports were rejected due to digital evidence being considered invalid. Finally, the dominance of large e-commerce platforms places half of the respondents in a disadvantaged position, as dispute resolution is largely governed by internal platform policies rather than formal legal norms, further reinforcing the structural vulnerability of MSMEs to digital fraud.

2. Inter-Agency Coordination Model

The integration of normative findings from positive legal analysis and empirical findings from in-depth interviews has led to the development of a coordination model design, which can serve as a framework for countering digital fraud among market traders and Banjarmasin MSMEs.[21] This model is built with a three-pillar approach that complements each other.

At the institutional and regulatory level, the model places law enforcement as the core structural foundation, with cyber officers serving as the frontline. They have the formal authority to follow up on digital fraud reports, using Article 492 of the New Criminal Code as a legal basis.[22] However, for the implementation of this task to be effective, the apparatus must obtain full support, including quick access to transaction data controlled by digital platforms. Without data disclosure from the platform, the authorities will always face obstacles in the proof process. Therefore, it is essential to establish a memorandum of understanding (MoU) between law enforcement authorities and platform providers to enable data sharing to occur efficiently, lawfully, and with due protection of consumer confidentiality.

From a capacity-building perspective, improving legal and digital literacy becomes an equally crucial component of the coordination model. This coordination model emphasises that legal protection will not be adequate if market traders and MSMEs remain in a state of legal blindness and low digital

[21] Adriana Tiron-Tudor, Widad Atena Faragalla, and Anca Pianoschi, "The role of the accountancy professionals in detecting and preventing fraud, in a digital landscape: a systematic literature review," *Digital Finance* (2025): 12

[22] Nur Hadiyati, and Hayllen Stathany, "Analisis Undang-Undang ITE Berdasarkan Asas Pembentukan Peraturan Perundang-Undangan Di Indonesia," *Mizan: Jurnal Ilmu Hukum* 10, no. 2 (2021): 149. See too, Yanus Sumitro, Fachrudy Asj'ari, Tri Ariprabowo, Ferry Hariawan, Martha Suhardiyah, and Bayu Adi, "Edukasi Keamanan Digital Untuk UMKM Guna Pencegahan Penipuan Dan Perlindungan Data Usaha," *Ekobis Abdimas: Jurnal Pengabdian Masyarakat* 6, no. 1 (2025): 126.

literacy.[23] Therefore, integrated training needs to be carried out by involving the Ministry of Cooperatives and SMEs, local governments, market associations, and law enforcement officials. The training focuses not only on technical skills such as transaction security or digital account management, but also on a substantive understanding of traders' legal rights, reporting mechanisms, and criminal consequences of digital fraud practices. In this way, legal and digital literacy can run in parallel, strengthening the capacity of traders in preventing and handling cases.[24]

To ensure operational effectiveness and public trust, the coordination framework is further reinforced through the development of an application-based integrated reporting system. One of the main obstacles found in the field is the low trust of traders to report fraud cases, as the process is considered convoluted and time-consuming. To address this issue, a local app-based reporting system was developed, making it easily accessible via smartphone. This application is equipped with a report status tracking feature so that reporters can monitor the progress of cases transparently. With this system in place, traders feel more confident that their reports will not stop at the administrative table, but are actually processed to the investigation and enforcement stage.

The results of the limited trial show the great potential of this three-pillar coordination model. Some traders who try the digital reporting system say they feel more confident in reporting fraud cases, because there is certainty of follow-up that can be monitored directly. In fact, MSME associations report that the level of traders' participation in reporting has increased after this mechanism. This indicates that the coordination model has not only been successful in enhancing the institutional process of case handling, but has also been effective in transforming public legal attitudes and behaviors.

Thus, this three-pillar-based coordination model not only serves as a practical solution to regulatory and institutional barriers but also as a strategic effort in building a more responsive, participatory, and equitable digital criminal law ecosystem. This model can serve as a prototype for regions facing similar challenges in protecting small businesses from digital fraud.

[23] Mohammad Daffa Saifullah, and Agus Pramono, "Penegakan hukum tindak pidana penipuan online: studi implementasi undang-undang ite di Indonesia," *Jurnal Magister Hukum Perspektif* 16, no. 2 (2025): 135.

[24] Aina Aurora Mustikajati, and Sulistyanta Sulistyanta, "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Berdasarkan Perspektif KUHP dan Undang-Undang Informasi dan Transaksi Elektronik," *Politika Progresif: Jurnal Hukum, Politik dan Humaniora* 1, no. 2 (2024): 156. See too, Andrew Phippen, Digital Literacy, In *Encyclopedia of Libraries, Librarianship, and Information Science*, (Amsterdam: Elsevier, 2025), 125.

3. Testing the Digital Fraud Decrease

The central findings in this study states that the synergy between actors, including law enforcement officials, digital platforms, MSME associations, and market traders, can make a real contribution to reducing the rate of digital fraud. The validity of this result is evident from the empirical data that were successfully collected during the limited trial period.

Before the implementation of the coordination model, the average number of digital fraud cases reported in Banjarmasin reached 10 cases per month. This figure is relatively consistent and reflects a fairly high level of vulnerability among market traders and MSMEs. However, after six months of implementation of the three-pillar-based coordination model, the average number of cases decreased to 7 cases per month. This 30% decline is not only statistically significant, but also socially and legally significant. This shows that when the coordination mechanism is activated, there is a tangible impact on the level of digital crime experienced by market traders.

This decline can be explained through several mechanisms. First, there is a deterrent effect. Digital fraudsters have become more cautious because they realise that the reporting mechanism has been integrated with cyber apparatus, so the risk of being caught increases. Second, increased legal awareness among traders makes them more vigilant and able to recognise fraud patterns, thanks to legal and digital literacy training organised within the framework of a coordination model.[25] Third, the presence of an application-based reporting system with a tracking feature increases traders' trust in the authorities, so that the number of incoming reports is more representative. As a result, the authorities can intervene more quickly, thereby reducing the likelihood of similar cases recurring.

Academically, these findings are in line with the theory of deterrence in criminal law, which emphasises the importance of legal certainty and enforcement effectiveness as factors that can reduce the intensity of crime.[26] Synergy between actors has been proven to not only create legal certainty but also strengthen prevention capacity at the community level. This shows that the effectiveness of criminal law is not only determined by the articles in the Criminal Code, but also by how the article is operationalised through cross-agency coordination.

---

[25] Nidhi Bansal, and Heena Choudhary, "Fostering digital equity: evaluating impact of digital literacy training on internet outcomes in rural marginalised communities in India," *International Journal of Lifelong Education* 43, no. 5 (2024): 483. See too, Winda Fitri, "The Legal Protection for Security Crowdfunding Based on Sharia Investment in MSMEs Economic Recovery," *International Journal of Law Reconstruction* 7, no. 1 (2023): 42.

[26] Thom Brooks, *Deterrence*, (Oxfordshire: Routledge, 2019). See too, Apitta Fitria Rahmawati, and Yuris Tri Naili, "Penguatan Literasi Digital dan Kesadaran Hukum Pidana Bagi UMKM Sebagai Kaum Rentan Terhadap Kejahatan Siber Berbasis AI di Wilayah Banyumas," *Jurnal Pengabdian Masyarakat-PIMAS* 4, no. 4 (2025): 407.

However, although the trial results show a positive trend, this study also identified limitations that require attention. The cost of developing and maintaining an application-based reporting system is quite high, so long-term sustainability still needs to be considered. Moreover, the reluctance of some traders to adopt digital technology remains a challenge, as not all of them possess sufficient skills or access to the necessary tools. Another contributing factor is the limited commitment of certain digital platforms, which are hesitant to grant access to transaction data in order to protect their business reputation and safeguard consumer confidentiality.

Table 3. Comparison of the Number of Digital Fraud Cases (Banjarmasin, 6 Months)

Period	Average Number of Cases/Month	Percentage Change
Before the coordination model	10	-
After the coordination model	7	-30%

Table 3 presents a comparison of the number of digital fraud cases experienced by market traders and MSMEs in Banjarmasin during two distinct periods: before and after the implementation of the three-pillar-based coordination model. The data provides a reasonably clear picture of the real impact of cross-agency coordination on reducing the rate of digital crime.

In the period before the coordination model was implemented, the average number of reported digital fraud cases reached 10 cases per month. This figure highlights the high level of vulnerability of MSME actors to digital fraud practices, indicating that existing legal protection mechanisms have been ineffective in providing a sense of security.

However, after the coordination model was tested on a limited basis for six months, the average number of cases dropped to 7 cases per month. Thus, there was a decrease of 30% compared to the previous period. This decline is not just a difference in numbers, but has an important substantive meaning. First, this data shows that the coordination model can improve the flow of case handling, from reporting to action, thereby encouraging a deterrent effect. Second, the reduction in fraud cases also shows an increase in legal awareness and vigilance of traders after participating in legal and digital literacy training.[27] Third, the transparency of the app-based reporting system encourages more

[27] Peng Li, Qinghai Li, and Shanxing Du, "Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China," *International Review of Economics & Finance* 91 (2024): 368. See too, Yuni Yuni Kristania Purba, and Roida Roida Nababan, "Perlindungan Hukum Bagi Korban Tindak Pidana Penipuan Pada Media Sosial," *Judge: Jurnal Hukum* 6, no. 04 (2025): 847.

traders to dare to report cases, which ultimately speeds up the response of the authorities to potential fraud.

Nonetheless, this decline must also be understood in a critical framework. The figure of 7 cases per month still shows that digital fraud cannot be eliminated. This indicates that the coordination model, although effective in reducing the number of cases, still needs further strengthening in order to provide optimal protection. Factors such as the sustainability of funding, ongoing resistance from merchants with low levels of digital literacy, and the limited commitment of major e-commerce platforms are key variables in determining whether this downward trend can be maintained over the long term.

Overall, Table 3 confirms that the three-pillar-based coordination model has great potential in reducing digital crime rates, as well as proving that the research regarding the effectiveness of synergies between actors is true. The 30% decrease in a relatively short time is an early indicator that normative and empirical integration can produce policies that are applicable and have a direct impact on small business actors in Banjarmasin.

The findings of this study clearly underline that the existence of regulations in the form of written norms, such as Article 492 of the New Criminal Code, is not enough to guarantee the effectiveness of legal protection against digital fraud practices. Criminal law, in this context, cannot stand alone as an abstract normative text, but rather must be supported by a precise, operational, and multi-stakeholder coordination mechanism. Without cross-agency coordination, regulations risk becoming just a dead letter law that has no practical relevance in the field.[28]

Article 492 of the New Criminal Code has indeed provided a legal basis, but to make it a truly effective instrument, more detailed derivative rules are needed. This derivative rule is important, for example, to regulate standards for the recognition of electronic evidence as legitimate evidence, a mechanism for the division of authority between cyber apparatus and digital platforms, and procedures for accelerating case handling. Without these technical arrangements, law enforcement officials will still face difficulties in integrating the provisions of the New Criminal Code with the ITE Law, especially in the aspect of electronic evidence. In other words, the successful implementation of Article 492 will largely depend on the extent to which derivative regulations can close the current regulatory gap.

Empirically, this study confirms that legal and digital literacy are the main foundations that determine the ability of market traders to protect

[28] Daniel Danglades, and Emmanuelle Laudic-Baron, "Navigating criminal justice cooperation: A French perspective on EU framework decisions," *European Journal of Probation* 16, no. 1 (2024): 96.

themselves from online fraud. Legal literacy provides an understanding of rights and obligations, as well as legal procedures that can be taken when becoming a victim. Meanwhile, digital literacy equips traders with the technical skills to recognise, prevent, and address technology-based fraud modes. Without these two aspects, the legal protections available will be difficult for legal subjects who should be the primary beneficiaries to take advantage of.

From an academic perspective, this research makes a significant contribution by expanding the study of criminal law at the micro level. So far, the discourse of digital criminal law has more often focused on large-scale or corporate cases, while market traders and MSMEs tend to be ignored.[29] Instead, this research highlights groups that have been on the margins and thus enriches the academic literature with a more inclusive perspective. This approach shows that criminal law is not only relevant for large entities, but must also be present to protect vulnerable groups in the economic structure of the Community.[30]

Practically, the three-pillar coordination model produced by this research can be used as a reference for policy formulation, both at the regional and national levels. This model not only serves as a short-term solution but can also be adapted as a long-term strategy to build a responsive and participatory digital criminal law ecosystem. If adopted consistently, this model has the potential to strengthen legal protection, increase public trust in the authorities, and reduce the rate of digital fraud among MSMEs. Thus, this research not only makes a theoretical contribution but also presents relevant practical implications for the development of criminal law in the digital era.

D. CONCLUSION

This research demonstrates that Article 492 of the New Criminal Code has not yet functioned optimally as a protective legal instrument for market traders and MSMEs facing digital fraud. The ineffectiveness of this provision is not rooted in normative deficiencies alone, but rather in structural and practical constraints, particularly low levels of digital literacy, limited access to legal information, weak coordination between traders and law enforcement authorities, and the dominant position of large e-commerce platforms in dispute resolution. These interrelated vulnerabilities collectively reduce the capacity of MSMEs to prevent, report, and resolve digital fraud cases effectively. Legal norms require supporting mechanisms that enable their

[29] Arben Prifti, "The impact of digital transformation to the criminal law assets." In *International Conference "New Technologies, Development and Applications"*, (Cham: Springer Nature Switzerland, 2024), 52.

[30] Agne Limante, "Protecting vulnerable groups in Europe: highlights from recent case law of the European Court of Human Rights," *The International Journal of Human Rights* 28, no. 4 (2024): 676.

practical enforcement and accessibility at the grassroots level. The coordination model developed in this study based on law enforcement support, enhanced digital and legal literacy, and an application-based integrated reporting system has empirically demonstrated its capacity to reduce digital fraud cases by up to 30% within a six-month trial period. This measurable impact underscores the strategic value of collaborative governance in addressing cybercrime risks affecting vulnerable economic actors.

The urgency of this research lies in its policy and practical implications. As digitalization of MSMEs continues to accelerate, unresolved structural vulnerabilities will expose small traders to increasing risks of economic loss and legal marginalization. Without immediate efforts to strengthen inter-stakeholder synergy, digital fraud may undermine trust in digital markets and slow MSME digital adoption. Therefore, this study provides an essential evidence-based foundation for policymakers, law enforcement agencies, and digital platforms to design more inclusive, responsive, and enforceable legal protection frameworks for MSMEs in the digital era.

BIBLIOGRAPHY

Journals:

Abdrasulov, Ermek, Akmaral Saktaganova, Indira Saktaganova, Sayash Zhenissov, and Zhassulan Toleuov. "Legal awareness and its significance when determining the nature of a person's legal behaviour." *International Journal of Electronic Security and Digital Forensics* 15, no. 6 (2023): 578-590.

Ausat, Abu Muna Almaududi. "In-depth study of the strategic interaction between electronic commerce, innovation, and attainment of competitive advantage in the context of SMEs." *International Journal of Analysis and Applications* 23 (2025): 78-78.

Bakhtiar, Handar Subhandi, Amir Ilyas, Abdul Kholiq, and Handina Sulastrina Bakhtiar. "The utilisation of scientific crime investigation methods and forensic evidence in the criminal investigation process in Indonesia." *Egyptian Journal of Forensic Sciences* 15, no. 1 (2025): 39.

Bansal, Nidhi, and Heena Choudhary. "Fostering digital equity: evaluating impact of digital literacy training on internet outcomes in rural marginalised communities in India." *International Journal of Lifelong Education* 43, no. 5 (2024): 473-493.

Danglades, Daniel, and Emmanuelle Laudic-Baron. "Navigating criminal justice cooperation: A French perspective on EU framework decisions." *European Journal of Probation* 16, no. 1 (2024): 93-104.

Efendi, Sahlan, Hendra Sukarman, Iwan Setiawan, and Muhammad Amin Effendy. "Analisis tindak pidana penipuan pasal 378 undang-undang nomor 1 tahun 1946 dibandingkan dengan pasal 492 undang-undang nomor 1 tahun 2023." *Pustaka Galuh Justisi* 3, no. 2 (2025): 179-195.

Fan, Di, Andy CL Yeung, Daphne W. Yiu, and Chris KY Lo. "Safety regulation enforcement and production safety: The role of penalties and voluntary safety management systems." *International Journal of Production Economics* 248 (2022): 108481.

Fitri, Winda. "The Legal Protection for Security Crowdfunding Based on Sharia Investment in MSMEs Economic Recovery." *International Journal of Law Reconstruction* 7, no. 1 (2023): 39-53.

Grey, Colin. "Bureaucracy without alienation." (2020): 126-143.

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): 146-156.

Indrawati, Nur Khusniyah, Sri Muljaningsih, Himmiyatul Amanah Jiwa Juwita, A. Muhamad Jazuli, Nuraini Desty Nurmasari, and Mochammad Fahlevi. "The mediator role of risk tolerance and risk perception in the relationship between financial literacy and financing decision." *Cogent Business & Management* 12, no. 1 (2025): 2468877.

Li, Peng, Qinghai Li, and Shanxing Du. "Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China." *International Review of Economics & Finance* 91 (2024): 364-377.

Limante, Agne. "Protecting vulnerable groups in Europe: highlights from recent case law of the European Court of Human Rights." *The International Journal of Human Rights* 28, no. 4 (2024): 671-688.

Lisma, Lisma. "Progressive law functions in realizing justice in Indonesia." *Syariah: Jurnal Hukum dan Pemikiran* 19, no. 1 (2019): 1-14.

Mustikajati, Aina Aurora, and Sulistyanta Sulistyanta. "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Berdasarkan Perspektif KUHP dan Undang-Undang Informasi dan Transaksi Elektronik." *Politika Progresif: Jurnal Hukum, Politik dan Humaniora* 1, no. 2 (2024): 156-169.

Nugroho, C., A. Wulandari, D. Maulana, N. Rina, and A. F. Kalaloi. "Digital communication and literacy for MSME empowerment: Evidence from a rural digital village in Indonesia." *International Journal of Innovative Research and Scientific Studies* 8, no. 3 (2025): 4523-4535.

Park, Sora, J. Ramon Gil-Garcia, Theresa A. Pardo, Megan Sutherland, and Andrew Roepe. "Cross-boundary information sharing in regulatory contexts: The case of financial markets." *Public Money & Management* 39, no. 5 (2019): 346-354.

Purba, Yuni Yuni Kristania, and Roida Roida Nababan. "Perlindungan Hukum Bagi Korban Tindak Pidana Penipuan Pada Media Sosial." *Judge: Jurnal Hukum* 6, no. 04 (2025): 845-853.

Putra, Muhammad Ardiansyah Satria Dwi, and Ifahda Pratama Hapsari. "Implikasi Sanksi Pemidanaan di Dalam KUHP Baru Terhadap Delik Penipuan Transaksi Secara Online." *UNES Law Review* 7, no. 3 (2025): 1063-1070.

Putri, Dina Elisa, Elly Sudarti, and Elizabeth Siregar. "Tindak Pidana Penipuan Melalui Aplikasi Digital (Gagasan Pemikiran Pertanggungjawaban Oleh Bank)." *PAMPAS: Journal of Criminal Law* 5, no. 1 (2024): 72-87.

Putri, Ni Kadek Marlita Erdiana, Kadek Januarsa Adi Sudharma, AA Ayu Ngurah Sri Rahayu Gorda, and AA Ayu Intan Puspadewi. "Kebijakan Yuridis dan Implementasi Perlindungan Konsumen Bitcoin dalam Menghadapi Ancaman Penipuan Online di Indonesia." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3, no. 4 (2025): 3912-3923.

Rahmawati, Apitta Fitria, and Yuris Tri Naili. "Penguatan Literasi Digital dan Kesadaran Hukum Pidana Bagi UMKM Sebagai Kaum Rentan Terhadap Kejahatan Siber Berbasis AI di Wilayah Banyumas." *Jurnal Pengabdian Masyarakat-PIMAS* 4, no. 4 (2025): 400-409.

Rustam, Martha Hasanah, Hamler Hamler, Tat Marlina, Duwi Handoko, and Rahmad Alamsyah. "Peran dan tanggung jawab konsumen untuk mencegah praktik penipuan dalam transaksi online dari perspektif hukum perlindungan konsumen." *Riau Law Journal* 7, no. 1 (2023): 1-24.

Saifullah, Mohammad Daffa, and Agus Pramono. "Penegakan hukum tindak pidana penipuan online: studi implementasi undang-undang ite di indonesia." *Jurnal Magister Hukum Perspektif* 16, no. 2 (2025): 130-140.

Sumitro, Yanus, Fachrudy Asj'ari, Tri Ariprabowo, Ferry Hariawan, Martha Suhardiyah, and Bayu Adi. "Edukasi Keamanan Digital Untuk UMKM Guna Pencegahan Penipuan Dan Perlindungan Data Usaha." *Ekobis Abdimas: Jurnal Pengabdian Masyarakat* 6, no. 1 (2025): 123-132.

Tiron-Tudor, Adriana, Widad Atena Faragalla, and Anca Pianoschi. "The role of the accountancy professionals in detecting and preventing fraud, in a digital landscape: a systematic literature review." *Digital Finance* (2025): 1-42.

Tsai, Fu-Ching. "The application of blockchain of custody in criminal investigation process." *Procedia Computer Science* 192 (2021): 2779-2788.

Wahid, Abdul. "Measuring the Effectiveness of the New Criminal Code in Answering Contemporary Criminal Law Challenges." *Lex Journal: Kajian Hukum Dan Keadilan* 9, no. 1 (2025): 47-57.

Wangmo, Tenzin, Veerle Provoost, and E. Mihailov. "The vagueness of integrating the empirical and the normative: Researchers' views on doing empirical bioethics." *Journal of Bioethical Inquiry* 21, no. 2 (2024): 295-308.

Wulandari, Cahya, Sugianto Sugianto, Anggyi Trisnawan Putra, Zidney Ilma Fazaada Emha, and Muhamad Sayuti Hassan. "Literacy, Compliance, and Digital Legal Awareness: The Role of JDIH UNNES in Disseminating Legal Information." *Indonesian Journal of Advocacy and Legal Services* 7, no. 1 (2025): 233-254.

Wulandari, Siti Sri, Mohd Lizam Bin Mohd Diah, and Andi Asari. "Digital proficiency and entrepreneurial mindset for sme success through market savvy and tech literacy." *Aptisi Transactions on Technopreneurship (ATT)* 7, no. 1 (2025): 26-36.

Yanto, Heri, Niswah Baroroh, Ain Hajawiyah, and Nurhazrina Mat Rahim. "The Roles of entrepreneurial skills, financial literacy, and digital literacy in maintaining MSMEs during the COVID-19 Pandemic." *Asian Economic and Financial Review* 12, no. 7 (2022): 504.

Books:

Akhtar, Saeed, and Siba Borah, Prasad. *Regulatory Frameworks and Digital Compliance in Green Marketing*. Hershey: IGI Global, 2025.

Brooks, Thom. *Deterrence*. Oxfordshire: Routledge, 2019.

Lestari, Mey Richa Madya. *Methods of Teaching Arabic*. Omsk: Economic of Region, 2009.

Phippen, Andrew. Digital Literacy. In *Encyclopedia of Libraries, Librarianship, and Information Science*. Amsterdam: Elsevier, 2025.

Conference:

Pandit, Kanika, and Renu Mahajan. "Advancing Digital Forensics: Harnessing Blockchain for Evidence Authentication." In *2024 Second, International Conference on Advanced Computing & Communication Technologies (ICACCTech)*. IEEE, 2024.

Prifti, Arben. "The impact of digital transformation to the criminal law assets." In *International Conference "New Technologies, Development and Applications."* Cham: Springer Nature Switzerland, 2024.