Journal of Legal and Cultural Analytics (JLCA)
Vol. 5, No. 3, 2026 : 421 - 436

JLCA

Imitation of MSME Transaction Documents as a Form of Business Identity Misuse: A Socio-Legal Analysis of the Gap Between Norms and Practices

Eghi Hendri Rifaldo Purba[1*], Martono Anggusti[2], Samuel Frans Boris Situmorang[3]
Fakultas Hukum, Universitas HKBP Nomensen
martono.anggusti@uhn.ac.id, samuel.situmorang@uhn.ac.id
Corresponding Author: Eghi Hendri Rifaldo Purba eghipurba@student.uhn.ac.id

A R T I C L E I N F O

Keywords: Business Identity, Transaction Document Forgery, Digital Identity Misuse, Socio-Legal, Legal Gap

Received : 01 June 2026
Revised : 05 July 2026
Accepted: 08 August 2026

A B S T R A C T

The counterfeiting of Micro, Small, and Medium Enterprise (MSME) transaction documents—a form of business identity misuse—is a crime that has emerged alongside the accelerated digital transformation of economic activities. This study aims to comprehensively analyze the gap between legal norms (*das sollen*) and social practices (*das sein*) regarding the protection of MSME business identities, employing a socio-legal approach. The research methodology combines a normative-juridical approach with a socio-legal perspective. This approach views law not merely as written norms ("law in the books") but also as social practices operating within society ("law in action"). Research data were gathered through a literature review of primary, secondary, and tertiary legal materials, alongside an analysis of digital transaction document usage patterns within the MSME ecosystem. The findings reveal a significant legal gap in the protection of MSME business identities in the digital era. Normatively, Indonesian law provides instruments to address document forgery and the manipulation of electronic information. Empirically, however, the effectiveness of these measures is severely limited by the high costs associated with digital evidence, the complexity of electronic forensic processes, and the absence of an integrated, affordable, and easily accessible business identity verification system for MSME players. Consequently, existing legal protections remain largely formalistic and fail to fully address the needs of the small-scale economic community.

DOI : https://doi.org/10.55927/jlca.v5i3.17092
ISSN-E: 2961-807X
https://journal.formosapublisher.org/index.php/jlca

INTRODUCTION

Micro, Small, and Medium Enterprises (MSMEs) serve as an engine of growth for the Indonesian economy, contributing significantly to the national Gross Domestic Product (GDP). In the context of the digital economy, business identity is no longer confined to conventional aspects such as names and logos; it has transformed into a digital asset representing credibility, reputation, and consumer trust. However, this transformation has also given rise to new risks, specifically business identity theft—the misuse of a business's identity for illegal purposes. A growing form of this issue involves the imitation of transaction documents—such as invoices, receipts, and work orders—for use as instruments of fraud.

From a normative standpoint, the Indonesian legal system provides instruments to protect electronic documents and address the misuse of business identities, notably through Article 263 of the Criminal Code (KUHP) regarding document forgery and Article 35 of the Electronic Information and Transactions Law (UU ITE) regarding the manipulation of electronic information. The existence of these provisions reflects a legal expectation that digital transactions occur securely and that legal certainty is provided for business actors, including MSMEs.

In reality, however, MSME operators frequently encounter the misuse of their business identities through the imitation of invoices, bills, and other digital transaction documents. Documents used in MSME operations generally lack adequate electronic authentication systems, making them easily replicated and modified using simple digital tools. Furthermore, high costs associated with digital evidence, low levels of legal literacy, and limited access to law enforcement mechanisms hinder the effective realization of the legal protections that exist in theory.

This situation reveals a gap between legal expectations (*das sollen*) and the reality of social practice (*das sein*). While the law normatively recognizes and protects electronic documents, empirically, such protection has yet to meet the actual needs of MSME operators within the digital economy ecosystem. Consequently, this study employs a socio-legal approach to analyze the law's operation within social practice and to identify the factors preventing the effective legal protection of MSME business identities. Previous studies have generally addressed document forgery within general contexts or formal sectors such as banking. However, research specifically analyzing the imitation of transaction documents within the MSME ecosystem using a socio-legal approach remains limited. This is significant because the characteristics of MSMEs—specifically their limited resources regarding both technology and legal literacy—render them the group most vulnerable to the misuse of business identities.

From a sociological perspective, MSME operators face limited access to document security technologies, such as certified electronic signatures or adequate digital authentication systems. Consequently, transaction documents can easily be replicated using simple software. This situation creates serious challenges regarding legal proof, as formalistic evidentiary systems often fail to accommodate digital evidence that is simple yet factually relevant. Furthermore, low legal literacy and high litigation costs make MSME operators reluctant to pursue legal avenues, thereby widening the gap between normative law and social practice.

In light of these issues, this study offers a novel contribution by integrating normative analysis with a socio-legal approach to examine the protection of MSME business identities more comprehensively. The study not only examines applicable legal norms but also critiques the limitations of legal approaches that tend to be reactive rather than oriented toward preventive protection.

This study aims to:

(1) analyze the legal classification of the imitation of MSME transaction documents as a form of business identity misuse under Indonesian positive law;
(2) identify weaknesses in legal protection for MSMEs from a socio-legal perspective; and
(3) formulate a model for strengthening legal protection that is more inclusive, adaptive, and preventive.

The research employs a normative-juridical method supported by a socio-legal approach to analyze the interaction between legal norms and empirical realities in the field. The analysis reveals a significant legal gap, wherein formal evidentiary procedures fail to address the rapidly evolving and widespread methods of digital document imitation.

As a theoretical and practical contribution, this research proposes three pillars for strengthening legal protection. First, from a legal standpoint, it is necessary to develop the doctrine of business identity protection by adjusting evidentiary standards to be more adaptive to the nature of digital documents. Second, from a technical standpoint, the adoption of technology-based document authentication systems—such as encrypted Quick Response (QR) codes integrated with business databases—is required. Third, from a policy standpoint, it is necessary to develop Alternative Dispute Resolution (ADR) mechanisms that are more accessible to MSME players.

Thus, this research asserts that legal protection for MSME business identities cannot rely solely on a repressive approach; rather, it must be developed integratively by combining normative, technological, and sociological aspects to create a legal system responsive to the dynamics of the digital economy.

Problem Formulation

1. How does the legal framework address the imitation of MSME transaction documents as a form of business identity misuse under Indonesian positive law?
2. How can legal protection for MSME business identities be made effective in practice?

LITERATURE REVIEW

The development of digital economic activities has fundamentally changed the way Micro, Small, and Medium Enterprises (MSMEs) conduct transactions and establish business relationships. Electronic transactions increasingly rely on digital documents, electronic information, and digital identities as instruments of communication, evidence, and business legitimacy. Barkatullah (2019), Sutedi (2011), and Makarim (2020) emphasize the importance of electronic transactions and electronic documents within the contemporary legal system. From a socio-legal perspective, this development also changes the relationship between law and society because legal rules concerning electronic transactions must operate within rapidly changing technological and social environments. Friedman (2013) explains that the legal system cannot be understood solely through its formal rules but must also be examined through the interaction between legal institutions, legal substance, and society. Similarly, Rahardjo (2014) emphasizes that law should be understood in relation to social realities rather than merely as a collection of written rules. In the context of MSMEs, therefore, transaction documents should not be viewed merely as administrative records but also as instruments that contribute to business identity, trust, and legitimacy in digital transactions.

The increasing dependence on digital transaction documents also creates vulnerabilities involving document manipulation, identity misuse, and digital fraud. Hidayat and Mahardika (2022) identify vulnerabilities in the metadata of digital transaction documents that may be exploited in social engineering practices, while Kristianto and Arifin (2020) discuss the challenges of law enforcement in cases involving the counterfeiting of electronic documents in e-commerce transactions. The issue is further connected to digital identity theft and the protection of business-related information. Pradipta and Sinta (2022) examine the legal aspects of digital identity misuse, whereas Nugroho (2023) highlights the relationship between digital trust and business identity imitation within Indonesia's marketplace ecosystem. In the MSME context, Setyawati (2023) specifically discusses legal protection against digital invoice fraud, while Suwari Akhmadi et al. (2022) emphasize the broader need for legal protection of MSMEs in the digital era. These studies indicate that digitalization provides economic opportunities for MSMEs while simultaneously creating new forms of vulnerability. However, the existing literature tends to examine electronic transactions, personal data, digital identity, or particular forms of digital fraud separately, leaving room for a more integrated examination of the counterfeiting of MSME transaction documents as a form of business identity misuse.

METHODOLOGY

This study employs a socio-legal research methodology, an approach that examines law not merely as written norms ("law in the books") but also as social practice ("law in action"). This approach was selected because the issue under investigation relates not only to the dogmatic aspects of law but also to the effectiveness of norms within the socio-economic context of Micro, Small, and Medium Enterprises (MSMEs).

The study utilizes both a statute approach and a conceptual approach. The statute approach is used to analyze relevant legal norms, specifically provisions regarding document forgery and identity misuse under Indonesian positive law. Meanwhile, the conceptual approach is employed to examine concepts such as business identity protection, business identity theft, and the gap between legal norms and actual practice.

The object of this research consists of digital transaction documents—such as invoices, bills, and proof of payment—used by MSMEs in their business activities. The research focuses on the national digital transaction ecosystem, particularly interactions occurring via social media platforms and instant messaging applications, which are vulnerable to document impersonation and business identity misuse.

Data sources for this study comprise both secondary and primary data. Secondary data consists of legal materials, including:

(1) primary legal materials, such as Law Number 1 of 2024 concerning Amendments to the Law on Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 20 of 2008 concerning MSMEs, and the Criminal Code; and
(2) secondary legal materials, such as scholarly journals, textbooks, academic papers, and findings from previous research relevant to the sociology of law and cybercrime.

Primary data was obtained through observations of transaction document usage patterns across several MSME clusters, as well as through interviews or focused discussions with legal practitioners and/or representatives of MSME associations. This data is used to identify sociological barriers regarding the reporting and enforcement of laws concerning the misuse of business identities.

Data collection was conducted through a literature review and a study of documentation. The literature review involved cataloging and analyzing relevant legislation and academic literature. Meanwhile, the documentation study entailed analyzing the formats and structures of MSME transaction documents circulating within the digital ecosystem to identify metadata elements and vulnerabilities that could facilitate manipulation.

Data analysis was performed qualitatively using a descriptive-analytical approach. This analysis aimed to examine the relationship between legal norms and empirical realities, as well as to identify legal gaps in the protection of MSME business identities. The research is premised on the assumption that weaknesses in legal protection stem not merely from a lack of regulation, but from information asymmetry and economic barriers to accessing legal protection mechanisms and document security technologies.

Consequently, the analysis focuses on how the law should adapt—particularly regarding standards of proof and protection mechanisms—to become more responsive and equitable toward the needs of MSME operators, who are vulnerable to business identity misuse.

A socio-legal approach is employed in this study to identify and analyze the gap between law as an ideal norm (*law in the books* or *das sollen*) and law as a social practice (*law in action* or *das sein*). The analysis focuses on the extent to which legal provisions concerning electronic documents, document forgery, and business identity protection provide tangible protection for MSME operators in their day-to-day digital transactions.

RESEARCH RESULT AND DISCUSSION

1. The Legal Status of MSME Transaction Documents within the Evidentiary System and Their Vulnerability to Identity Misuse

From a normative standpoint, Indonesian law recognizes electronic documents as valid evidence under Article 5, paragraph (1) of the Electronic Information and Transactions Law (UU ITE). This provision reflects a legal intent to ensure that digital transactions enjoy the same legal certainty and protection as conventional transactions. Given this recognition, MSME transaction documents—such as bills, invoices, and electronic payment receipts—should serve as effective evidentiary instruments to safeguard the identities and legal interests of business owners. Furthermore, the existence of both conventional and cyber-related criminal provisions indicates that criminal law is expected to prevent document forgery and the manipulation of electronic information that could harm MSMEs within the digital economic ecosystem. In the evolution of Indonesian evidentiary law, MSME transaction documents have assumed an increasingly significant role, being legally classified as an extension of written evidence.

To address the forgery of transaction documents, Indonesia's positive legal system provides two clear, fundamental legal pillars. The first pillar is Article 263 of the Criminal Code (KUHP) regarding document forgery, which serves as the conventional substantive legal basis. This article stipulates that anyone who creates a false document or falsifies a document—where said document creates a right, an obligation, or a debt discharge, or serves as proof of a fact—with the intent to use it (or have others use it) as if it were authentic and unaltered, is liable for the crime of document forgery. In the context of MSMEs, items such as receipts, invoices, or physical and digital stamps are classified as documents capable of establishing rights or payment obligations; thus, their forgery satisfies the substantive elements of this article. The second pillar is Article 35 of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, which serves as the specific legal basis for cyber-related offenses. This article prohibits any person from intentionally and without authorization—or unlawfully—manipulating, creating, altering, deleting, or damaging Electronic Information and/or Electronic Documents with the intent of making such documents appear authentic. In the realms of e-commerce and instant messaging transactions, acts such as replicating digital invoices or manipulating proof-of-transfer records constitute clear examples of electronic document manipulation designed to deceive MSME operators into accepting them as authentic.

However, the evidentiary weight of such MSME digital documents varies. Documents bearing a certified electronic signature possess strong, binding evidentiary value, akin to that of an authentic deed. Conversely, transaction documents commonly used by MSMEs—which typically lack authentication or encryption systems—tend to be regarded merely as private deeds (*akta di bawah tangan*); in some instances, they serve only as preliminary evidence or circumstantial indicators. In practice, the majority of MSME operators still utilize simple transaction documents devoid of certified electronic authentication. These documents are generally created using standard applications and distributed via social media or instant messaging platforms without adequate security mechanisms. Consequently, these transaction documents are easily replicated, modified, and used to fabricate legitimacy in digital transactions. In many cases, MSME operators who fall victim to the misuse of their business identity face significant difficulties in proving that the documents were forged or used without their consent; furthermore, the high cost of digital forensic audits and the complexities involved in electronic evidence often render effective legal protection inaccessible to many MSME operators.

This disparity creates significant legal ambiguity: while the law recognizes electronic documents as valid evidence, not all documents possess equal evidentiary weight. From a socio-legal perspective, this situation reveals a gap between legal norms (*law in the books*) and actual document usage practices among MSMEs (*law in action*). The vulnerability of MSME transaction documents to identity misuse stems not merely from normative weaknesses but from the interplay of technical and sociological factors. These factors include the use of informal document distribution channels—such as easily replicated instant messaging apps—and low levels of legal and digital literacy among MSME operators, who often view documents merely as administrative tools. Additionally, weak third-party verification mechanisms create opportunities for manipulated documents to be used to legitimize illegal transactions. In practice, this situation imposes a disproportionate burden of proof on MSME operators; victims of identity misuse are often compelled to prove they did not engage in specific transactions—a task of "proving a negative" that constitutes a formidable evidentiary burden both theoretically and practically. This indicates that existing evidentiary systems have not fully adapted to the nature of digital documents within the small business ecosystem. The situation highlights a disconnect between legal expectations and social practices regarding the protection of MSME business identities. While the law normatively provides criminal sanctions for the forgery of digital documents, such protections remain empirically inaccessible to MSME operators due to economic, technological, and evidentiary capacity constraints. Regarding the legal structure—drawing on Lawrence M. Friedman's theory—law enforcement agencies still face technical capacity limitations when handling digital evidence at the micro-business scale. In practice, reports involving invoice impersonation are frequently dismissed as ordinary business losses rather than serious digital identity crimes, resulting in slow and unresponsive law enforcement processes. It is precisely the disconnect between the formalistic standards of criminal law and the culture of trust-based communal transactions that gives rise to an "access to justice gap," wherein the micro-economic class is unable to utilize positive legal instruments due to the costs of forensic procedures and technological limitations.

1.1. Socio-Legal Analysis of the Digital Evidence System for MSMEs

- Socio-Legal Analysis: The Gap Between "Law in the Books" and "Law in Action"

From a socio-legal perspective, legal effectiveness is measured not merely by the existence of written norms, but by how those norms function within social reality. Lawrence M. Friedman explains that the operation of law is influenced by three key elements: legal structure, legal substance, and legal culture. In the context of protecting MSME business identities, a lack of alignment among these three elements hinders the law's effectiveness.

Regarding legal substance, Indonesia possesses sufficient normative instruments to penalize perpetrators who forge transaction documents—whether through provisions on document forgery in Article 263 of the Criminal Code (KUHP) or the manipulation of electronic information under Article 35 of the ITE Law. However, these norms are grounded in a conventional paradigm of document protection and fail to fully accommodate the nature of MSME digital transactions, which are characterized by speed, informality, and reliance on social trust.

Regarding legal structure, law enforcement agencies face limitations in technical capacity when handling digital evidence at the micro-scale. In practice, reports concerning invoice forgery or the misuse of MSME business identities are often dismissed as ordinary business losses rather than recognized as serious forms of digital identity crime. Consequently, law enforcement processes tend to be sluggish and unresponsive to the victims' needs. Meanwhile, regarding legal culture, MSME operators generally lack awareness that transaction documents constitute a vital part of their business's legal identity requiring protection. A culture of informal transactions via social media and instant messaging apps reveals that business relationships are built more on personal trust than on formal legal verification mechanisms. This environment creates a social landscape highly vulnerable to document forgery and business identity theft.

Thus, within a socio-legal framework, the core issue is not an absence of law, but rather the legal system's inability to adapt to social realities and the evolution of digital technology—developments that outpace the creation of regulations.

- A Socio-Legal Analysis of the Burden of Digital Proof for MSMEs

Theoretically, the criminal and civil evidentiary systems in Indonesia still prioritize formal proof as the primary instrument for establishing the validity of a document. In the context of MSME transactions, this situation creates an imbalance, as most business operators utilize simple documentation lacking certified electronic authentication. From a socio-legal perspective, the matter of proof is not merely a technical legal issue but also one concerning access to economic and technological resources. MSME operators generally lack the financial means to conduct digital audits, electronic forensic examinations, or secure professional legal counsel. Consequently, while they are normatively entitled to legal protection, realizing this right proves difficult in practice.

This phenomenon highlights an "access to justice" gap—a situation where the law exists formally but remains effectively inaccessible to certain segments of society. In the context of this study, MSMEs are the group most significantly affected, given their vulnerable economic and technological positions. Furthermore, current digital evidentiary systems tend to prioritize formal authentication methods, such as certified electronic signatures. Yet, in the social reality of MSME transactions, the validity of business relationships is often established through informal communication, transaction histories, and bonds of trust. This misalignment between formal evidentiary standards and actual social practices reveals a chasm between legal rationality and the economic realities faced by the community.

Theoretically, the evidentiary systems in Indonesian criminal and civil law still prioritize formal proof as the primary instrument for establishing the validity of a document. In the context of MSME transactions, this situation creates an imbalance, as the majority of business operators utilize simple documentation lacking certified electronic authentication. From a socio-legal perspective, the matter of proof is not merely a technical legal issue but also one concerning access to economic and technological resources. Generally, MSME operators lack the financial capacity to undertake digital audits, electronic forensic examinations, or secure professional legal counsel. Consequently, while they possess a normative right to legal protection, realizing that right in practice proves difficult. This phenomenon illustrates an "access to justice gap"—a situation where the law exists formally but remains effectively inaccessible to specific segments of society. In the context of this study, MSMEs are the group most significantly affected, given their vulnerable position in both economic and technological terms. Furthermore, current digital evidentiary systems tend to prioritize formal authentication methods, such as certified electronic signatures. Yet, in the social reality of MSME transactions, the validity of business relationships is frequently established through informal communication, transaction histories, and relationships built on trust. This misalignment between formal evidentiary standards and social practices reveals a chasm between legal rationality and the economic realities faced by the community.

2. Analysis of the Ineffectiveness of Legal Protection for MSME Business Identities in Practice

In practice, legal protection for MSME business identities has not functioned effectively due to a stark disconnect between formalistic regulations and the sociological realities of business operators. Substantively, although Law Number 1 of 2023 concerning the Criminal Code (KUHP) addresses the criminal offenses of document forgery (Article 391) and fraud (Article 492), implementation at the micro-enterprise level continues to face major obstacles regarding evidentiary requirements and law enforcement priorities. Empirical evidence from the field indicates that the imitation of physical transaction tools—such as stamps and receipt formats—used by [Name of Parents' Shop] is often dismissed by authorities as a minor infraction; yet, for MSME operators, these tools represent vital intellectual assets that embody their business reputation (goodwill). This ineffectiveness becomes even more apparent when viewed in light of Law Number 1 of 2024 regarding the Second Amendment to the ITE Law, specifically Article 35 concerning the manipulation of electronic information or documents. In an increasingly digital transaction landscape, manipulated transaction receipts distributed electronically ought to be protected; however, the complexity of digital forensic procedures and high data certification costs render these legal provisions inaccessible to MSMEs facing technological and financial constraints.

Furthermore, the application of Law Number 30 of 2000 on Trade Secrets has failed to provide optimal protection for MSMEs due to the "efforts to maintain secrecy" standard mandated by Article 3. The inherently open and informal sociological nature of MSMEs means they often lack internal protection mechanisms—such as Non-Disclosure Agreements (NDAs) or rigid data security systems—causing business identities featured on stamps and receipts to be legally deemed part of the public domain during disputes. This situation is exacerbated by the trademark registration system under Law Number 20 of 2016, which adheres to the "first-to-file" principle; this leaves MSMEs legally vulnerable, as they are often outpaced administratively by parties acting in bad faith. The gap between high-cost legal norms and the economic reality of MSMEs creates a scenario where the law exists merely as text ("law in books") rather than serving as a tangible solution ("law in action"). The complaint-based nature of law enforcement ultimately fosters apathy among MSME operators, as the cost of litigation in the Commercial Court often far exceeds the value of the actual financial loss incurred; consequently, protecting MSME business identities remains a significant challenge within the national legal system.

2.1 Socio-Legal Analysis of the Concept of Justice for MSMEs

In conventional legal approaches, justice is often understood as resolution through litigation mechanisms and the punishment of offenders. However, from a socio-legal perspective, justice must be understood more substantively—specifically, the extent to which the law can restore the social and economic conditions of the victim. For MSME operators, the primary need is not merely the punishment of the offender, but rather the restoration of business reputation, the rapid cessation of identity misuse, and the recovery of consumer trust. Consequently, restorative justice approaches and expedited administrative mechanisms are more relevant than lengthy and costly litigation processes.

This indicates that the concept of justice within the MSME ecosystem must shift from punitive justice toward restorative and responsive justice. The law must do more than simply punish after a loss has occurred; it must also be capable of preventing, detecting, and remedying losses in a rapid and proportionate manner.

3. Systemic Strategies to Close Loopholes Regarding Business Identity Misuse

This research demonstrates that the misuse of business identities cannot be addressed solely through penal approaches. A systemic strategy encompassing regulatory, technological, and legal-cultural aspects is required.

From a regulatory standpoint, it is necessary to develop a legal framework that specifically governs digital business identities, including minimum security standards for transaction documents. Standardizing electronic-based national transaction documents is crucial for ensuring uniformity and enhancing the reliability of evidence. From a technological perspective, the integration of national data systems is key. Developing a verification system based on a "single source of truth"—linked to business licensing, population registry, and tax data—enables real-time business identity verification. Implementing authentication technologies, such as dynamic verification codes, can also significantly reduce the potential for document forgery. From an institutional perspective, a rapid response mechanism for identity misuse is needed, including integrated reporting systems and cross-sector notifications to financial institutions and digital platforms. This aims to immediately sever the economic chain of the crime. Indonesia's legal framework exhibits a sectoral approach to regulating digital aspects, wherein personal data protection, electronic information, and MSME empowerment operate in parallel, lacking normative integration regarding the concept of business identity as a unified legal entity. Consequently, a regulatory gap—specifically an integration vacuum—has emerged, which is exploited in the practice of forging transaction documents.

Table 1. Socio-Legal Analysis of Regulatory Gaps in MSME Digital Identity Protection

Legal Basis	**Normative Strength**	**Weaknesses & Regulatory Gaps**	**Socio-Legal Analysis (The Gap)**
Law No. 1 of 2024(Electronic Information and Transactions Law / ITE Law)	Recognizes electronic documents as valid legal evidence; regulates information manipulation (Article 35) and digital forgery.	Does not regulate *business identity*; focuses on information rather than business reputation. The evidentiary standards, particularly forensic requirements, are too high and complex.	**Inaccessible Law:** Effective for large corporations, but fails to adequately address *micro-fraud* because the cost of obtaining evidence is too high for MSMEs.
Law No. 27 of 2022(Personal Data Protection Law / PDP Law)	Regulates the obligations of data controllers; provides a comprehensive legal basis for the protection of individuals' personal data.	Focuses on individual data rather than business/MSME identities. It does not cover invoices, transaction documents, or commercial identity.	**Regulatory Blind Spot:** The state protects individuals as persons, but has yet to protect business units as independent digital identity entities.

Legal Basis	Normative Strength	Weaknesses & Regulatory Gaps	Socio-Legal Analysis (The Gap)
Law No. 20 of 2008(Micro, Small, and Medium Enterprises / MSME Law)	Provides a foundation for economic empowerment and legal protection for small business actors.	Does not regulate digital identity security, the protection of transaction documents, or aspects of *digital trust*.	**Policy Inconsistency:** The state promotes MSME digitalization downstream, but does not provide a *legal shield* against digital risks upstream.
Law No. 1 of 2023 in conjunction with Law No. 1 of 2026(Criminal Code / KUHP)	Modernizes criminal law and strengthens the codification of the new national criminal law system.	The concept of forgery remains based on the classical paradigm of physical documents. It has not yet adapted to *identity cloning* and *synthetic documents*.	**Technologically Lagging:** Normatively, the framework has been modernized; however, technologically, it remains behind in responding to the increasingly sophisticated evolution of cybercrime.

Finally, regarding the substantive legal aspect, enhancing legal and digital literacy among MSME players and the general public is a crucial factor. Without the awareness that transaction documents are legal assets requiring protection, regulatory and technological interventions will prove ineffective. From a normative standpoint, Indonesian law—specifically the ITE Law and the Criminal Code (KUHP)—is intended to provide protection against the manipulation of electronic documents and the misuse of business identities. However, in practice, these regulations remain rooted in a conventional document paradigm and do not yet specifically address the protection of digital business identities for MSMEs. Consequently, the law has lagged in adapting to the rapid evolution of digital transaction technologies within society.

Analytical Synthesis

The research findings confirm that the weakness in legal protection for MSME business identities stems not from a lack of legal norms, but rather from a misalignment between norms, technology, and social reality. Within a socio-legal framework, this gap demonstrates that the effectiveness of the law is heavily dependent on its ability to adapt to social practices and technological advancements.

Thus, future protection for MSME business identities must be established through an integrative approach that combines legal reform, technological innovation, and the strengthening of legal culture, thereby bridging the gap between "law in the books" and "law in action."

CONCLUSIONS AND RECOMMENDATIONS

Based on the analysis and discussion in this study, several key points are concluded as follows:

1. Legal Status and Vulnerability of MSME Transaction Documents
   - Normative Recognition of Evidence: Normatively (*law in the books*), the legal status of MSME transaction documents is validly recognized as an extension of written evidence under Article 5 paragraph (1) of the ITE Law; they also receive criminal law protection via Article 263 of the Criminal Code (regarding document forgery) and Article 35 of the ITE Law (regarding the manipulation of electronic information).
   - Asymmetry in Evidentiary Weight: In sociological reality (*law in action*), this legal protection suffers from fundamental weaknesses because most MSME transaction documents are informal and lack certified authentication (relying instead on instant messaging apps or social media).
   - Weak Evidentiary Value: In law enforcement practice, such simple documents tend to hold the status of merely "private writings" (*akta di bawah tangan*) or preliminary evidence, making them highly susceptible to identity misuse (fraudulent identity construction).
   - Access to Justice Gap: This vulnerability is exacerbated by the heavy burden of digital proof (high-cost verification), which compels victims to engage in "proving a negative." This creates a gap in access to justice for micro-entrepreneurs due to financial constraints and limited technological capacity.
2. Effectiveness of Business and Sectoral Regulations in Practice
   - Suboptimal Sectoral Regulations: The effectiveness of legal protection for MSME business identities through business and other sectoral regulations—such as the MSME Law, Trade Secrets Law, Trademark Law, and Personal Data Protection Law (PDP Law)—has proven suboptimal in actual social practice.
   - • Policy Inconsistency: This ineffectiveness stems from policies that focus excessively on the downstream aspects of market digitalization without providing a "legal shield" at the upstream level. • Regulatory Blind Spot: A legal gap exists wherein the Personal Data Protection (PDP)

Law protects only the data of natural persons, excluding the identities of micro-enterprise entities.

- Clash Between Sociological Characteristics and Formalistic Standards: The open and informal nature of MSMEs conflicts with the formalistic standards of business law. Examples include the requirement for "efforts to maintain confidentiality" under Article 3 of the Trade Secrets Law and the "first-to-file" principle in the Trademark Law. Consequently, physical and digital transaction instruments—such as business stamps and receipt formats—are easily claimed by third parties or deemed to have entered the public domain.
- Unpreparedness of Legal Structure and Culture: Law enforcement mechanisms are not yet equipped to integrate MSME trade reputation (goodwill) as a vital asset. Compounded by the high cost of commercial litigation, this creates a clash of legal cultures, resulting in the law remaining merely static text ("law in books") rather than evolving into a living, responsive instrument of protection within the context of the community's digital economic reality.

REFERENCES

Ali, Achmad. (2015). *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialprudence) Termasuk Interpretasi Undang-Undang (Legisprudence)*. Jakarta: Kencana.

Barkatullah, Abdul Halim. (2019). *Hukum Transaksi Elektronik sebagai Panduan dalam Beraktivitas di Dunia Maya*. Bandung: Nusa Media.

Dewi, S. D. (2021). "Urgensi Pelindungan Data Pribadi dalam Ekosistem Ekonomi Digital di Indonesia." *Jurnal Hukum & Pasar Modal*, 11(1), 45–62.

Dewi, Sinta Dewi. (2016). *Cyber Law: Perlindungan Privasi atas Data Pribadi dalam Internet Banking*. Bandung: Refika Aditama.

Friedman, Lawrence M. (2013). *Sistem Hukum: Perspektif Ilmu Sosial (The Legal System: A Social Science Perspective)*. Bandung: Nusa Media.

Harahap, M. Yahya. (2017). *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan*. Jakarta: Sinar Grafika.

Hidayat, T., & Mahardika, A. (2022). "Analisis Vulnerabilitas Metadata Dokumen Transaksi Digital terhadap Praktik Social Engineering." *Jurnal Keamanan Informasi dan Kriptografi*, 5(2), 15–27.

Irawan, A. D. (2021). "Tinjauan Socio-Legal terhadap Budaya Keamanan Data pada Pelaku Usaha Kecil Menengah di Indonesia." *Jurnal Masyarakat dan Hukum*, 6(1), 12–29.

Kristianto, A., & Arifin, R. (2020). "Tantangan Penegakan Hukum terhadap Pemalsuan Dokumen Elektronik dalam Transaksi E-Commerce." *Jurnal Kertha Semaya*, 8(9), 1345–1360.

Makarim, Edmon. (2020). *Notaris dan Transaksi Elektronik: Kajian Hukum tentang Cybernotary atau Electronic Notary*. Jakarta: PT RajaGrafindo Persada.

Mansur, Dikdik M. Aritonang & Elisatris Gultom. (2015). *Cyber Law: Suatu Pengantar*. Bandung: Refika Aditama.

Mertokusumo, Sudikno. (2013). *Hukum Acara Perdata Indonesia*. Yogyakarta: Cahaya Atma Pustaka.

Nugroho, S. S. (2023). "Digital Trust dan Risiko Peniruan Identitas Usaha dalam Ekosistem Marketplace Indonesia." *Jurnal Ekonomi dan Bisnis Digital*, 2(4), 1102–1118.

Pradipta, R., & Sinta, D. (2022). “Analisis Yuridis terhadap Penyalahgunaan Identitas Digital (Identity Theft) Berdasarkan Undang-Undang Perlindungan Data Pribadi.” *Jurnal Hukum Siber dan Teknologi*, 2(2), 88–105.

Rahardjo, Satjipto. (2014). *Ilmu Hukum*. Bandung: PT Citra Aditya Bakti.

Ramadhani, R. (2022). “Hambatan Sosiologis Implementasi Tanda Tangan Elektronik Tersertifikasi pada Sektor UMKM.” *Jurnal Penelitian Hukum De Jure*, 22(3), 355–370.

Setyawati, M. A. (2023). “Perlindungan Hukum bagi UMKM terhadap Penipuan Invoice Digital dalam Transaksi Lintas Batas.” *Jurnal Ius Quia Iustum Law*, 30(2), 210–231.

Sitompul, Josua. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.

Subekti, R. (2010). *Hukum Pembuktian*. Jakarta: Intermasa.

Sutedi, Adrian. (2011). *Hukum Transaksi Elektronik*. Jakarta: Alfabeta.

Suwari Akhmadi, dkk. (2022). *Perlindungan Hukum UMKM di Era Digital*. Jakarta: Gramedia Pustaka Utama.

Wahid, Abdul & Mohammad Labib. (2010). *Kejahatan Mayantara (Cyber Crime)*. Jakarta: PT RajaGrafindo Persada.

Wicaksono, B. A. (2024). “Relasi Kuasa dan Kepercayaan: Analisis Socio-Legal Transaksi Informal UMKM di Media Sosial.” *Jurnal Hukum Lingkungan dan Sosial*, 4(1), 50–68.