

Notarial Authentication of Electronic Consumer Agreements: A Layered Trust Model for Digital Justice

Dita Perwitasari¹, Budi Santoso², Yunanto³, Zainur Rahman⁴, Nurul Hikmah⁵

^{1,2,3}Faculty of Law, Universitas Diponegoro, Semarang, Indonesia

⁴Faculty Of Technology Management and Business, Universiti Tun Hussein Onn Malaysia, Malaysia

⁵Faculty of Law, Universitas Negeri Surabaya, Surabaya, Indonesia

Corresponding author: ditaperwitasari@students.undip.ac.id

Abstract

Electronic consumer agreements are legally recognized but remain vulnerable to identity manipulation, opaque standard terms, unverifiable consent, fragile evidence, data-processing risks, and weak access to remedies. Existing scholarship commonly treats electronic signatures, consumer protection, and cyber-notarial development separately, leaving an institutional gap concerning how legal authenticity can protect consumers without imposing notarial form on ordinary digital commerce. Using normative legal research with statutory, conceptual, doctrinal, and functional-comparative approaches, this article develops a selective five-layer model of notarial authentication for high-risk electronic consumer agreements. The model integrates identity verification, meaningful-consent confirmation, content-integrity preservation, disclosure certification, and redress-oriented evidence custody. Its novelty lies in conceptualizing notarial authentication not as signature validation or mandatory notarization, but as a proportional, consumer-centered, evidence-oriented, and preventive-justice mechanism. The framework is intended for transactions presenting heightened indicators such as significant value, long-term obligations, embedded financing, cross-border elements, sensitive data, or clauses limiting consumer rights. Properly designed safeguards can strengthen consumer autonomy, privacy and informational self-determination, equality for vulnerable users, and access to effective remedies while preserving the efficiency of ordinary online transactions. The article concludes that regulatory clarification, procedural standards, professional competence, and institutional coordination are necessary to make selective electronic notarial authentication a credible trust infrastructure for digital consumer justice.

Keywords: Notarial Authentication; Electronic Agreement; Consumer Protection; Digital Consumer Justice; Electronic Evidence.

A. INTRODUCTION

Digital consumer transactions have changed the basic posture of private law. A consumer may now enter into a binding agreement by clicking a button, scanning a quick-response code, accepting bundled terms, or using an electronic signature service without ever meeting the business actor or reading a paper document. This speed supports economic efficiency, but it also changes how consent is expressed and later proved (Muh. Ali Masnun, Dicky Eko Prasetyo, Mohd Badrol Awang, 2024). In conventional contracting, the law could rely on face-to-face negotiation, paper records, handwritten signatures, and identifiable intermediaries. In electronic contracting, the legal system must examine interface design, authentication architecture, data integrity, platform governance, information asymmetry, and the evidentiary life cycle of a digital record. The result is not merely a technical shift from paper to screen. It redistributes risk from the business actor and the platform to consumers, who often do not control the digital environment in which the agreement is created.

The legal problem becomes sharper when electronic agreements are used in consumer transactions. Consumer law is built on the premise that the consumer is structurally weaker than the trader, whether because of unequal bargaining power, limited information, lower ability to assess risk, or dependence on standard-form contracts (Sulistiyowati, Eny, Muh. Ali Masnun, 2025). In digital markets, this inequality is amplified by design. Consumers often encounter terms hidden in hyperlinks, expressed in dense language, updated unilaterally, or combined with algorithmic persuasion. Studies on digital fairness show that older consumer protection rules, many drafted before platform commerce became dominant, often struggle to

address the behavioural and technological conditions of contemporary online contracting (Durovic & Poon, 2023; Howells, 2020). Jurnal Suara Hukum scholarship similarly emphasizes that contemporary consumer protection must respond to information asymmetry, digital-market vulnerabilities, privacy risks, and limited access to effective dispute resolution (Kadir et al., 2024). The contract may appear formally consensual, but dark patterns, unclear disclosures, rapid checkout flows, or technological dependence may affect its formation.

Cyber law responds to a different but related set of concerns. It asks whether electronic information, electronic documents, electronic signatures, electronic systems, and electronic certification services can create valid legal consequences. At the international level, the UNCITRAL Model Law on Electronic Commerce was designed to remove formal obstacles to electronic commerce by promoting equal treatment between paper-based and electronic information (UNCITRAL, 1996). The UNCITRAL Model Law on Electronic Signatures similarly emphasizes functional equivalence, reliability, and technology neutrality in evaluating electronic signatures (UNCITRAL, 2001). These instruments make electronic contracting possible, yet they do not fully answer the consumer protection question. A technically valid electronic signature may still be attached to an unfair contract. A reliable timestamp may still record consent given without information. A secure system may still impose non-negotiated terms on a consumer who did not understand the legal consequences.

Notarial law enters this discussion because notaries perform a preventive and evidentiary function in civil law. The notary is not merely a witness to signatures. The notary formalizes legal acts, verifies identity and capacity, explains legal consequences, records the intention of the parties, preserves authentic documents, and

produces evidence that carries high probative value. Indonesian notarial legislation frames the notary as a public official whose legal services contribute to certainty, order, and protection through authentic written evidence concerning legal acts, agreements, determinations, and events (Prasetio et al., 2025)(Republic of Indonesia, 2014). This public function is precisely what is threatened when consumer contracting becomes frictionless, remote, and difficult to verify. The question is therefore not whether notaries should resist digitalization, but how to redesign the notarial function so authenticity remains meaningful in the digital environment.

The tension lies between electronic validity and authentic form. Electronic transaction law generally recognizes that electronic information and electronic documents may have legal force. In contrast, notarial law continues to attach authenticity to deeds made by or before an authorized public official in accordance with legally prescribed form. Indonesian Government Regulation Number 71 of 2019 regulates electronic systems and electronic transactions, while Government Regulation Number 80 of 2019 governs trading through electronic systems (Republic of Indonesia, 2019a, 2019b). Law Number 1 of 2024 further updates Indonesia's electronic information and transaction regime (Republic of Indonesia, 2024). These instruments support digital transactions, but a doctrinal gap remains between ordinary electronic contracts and authentic deeds. If every electronic agreement is treated as sufficient without external authentication, consumers may lack strong evidentiary protection. If every digital transaction is forced into the old paper-based notarial form, innovation and access will suffer.

This article proposes a middle position. Notarial authentication should be understood as a selective trust layer for electronic consumer agreements, especially

where the transaction is high-value, high-risk, cross-border, linked to financing, involves long-term obligations, or contains clauses that may affect fundamental consumer rights. In such cases, the notary can bridge consumer protection and cyber law by validating not only the signature but also the integrity of the contractual process. This means the notary's role should include verifying identity, confirming informed consent, reviewing essential consumer disclosures, certifying the time and content of the agreement, and preserving an audit trail for use in court or alternative dispute resolution.

Previous research on electronic contracts has generally concentrated on the validity of electronic records, electronic signatures, or the evidentiary status of digital documents, while consumer-protection studies emphasize unfair standard terms, platform liability, data protection, and cross-border enforcement (Chen, 2023; Meskić, 2022; Wibowo, 2024). Cyber-notary scholarship, in turn, has focused on electronic deeds, certificate authorities, and digital signatures (Dewi, 2021; Prabhawisnu, 2023). Relevant Jurnal Suara Hukum studies strengthen this state of the art. Zamzam et al. (2023) examine the validity of electronic contractual relations in e-commerce together with legal responsibility for personal-data breaches; Wilbert et al. (2024) analyze the implications of the ASEAN Agreement on E-Commerce for electronic business contracts; Tsamara (2021) develops a comparative privacy and personal-data-protection perspective; Kadir et al. (2024) frame consumer protection reform around information, bargaining power, privacy, and access to justice; and Priyono et al. (2026) connect digital contract transformation with legal certainty and human-rights protection. These studies establish important but partial propositions: technical reliability can support legal validity; consumer law can police unfairness; privacy law

can constrain data processing; and notarial law can supply independent preventive and evidentiary authority. What remains unresolved is how to integrate these functions selectively in high-risk electronic consumer transactions. The distinctive value of the notary is institutional rather than merely technical: unlike a certification provider, the notary combines impartial legal counselling, capacity assessment, formalization, independent evidence custody, and public responsibility; unlike a platform, the notary is not the transaction designer; and unlike a court or consumer agency, the notary intervenes before a dispute crystallizes. The novelty of this article therefore lies not in proposing cyber notary in general, but in constructing a selective, consumer-centered, evidence-oriented, five-layer preventive-justice mechanism that allocates complementary responsibilities among notaries, platforms, certification providers, regulators, and dispute institutions.

The central research question is: how should notarial authentication be designed and institutionally allocated to strengthen fairness and evidentiary protection in high-risk electronic consumer agreements while remaining compatible with cyber law and notarial formality? Three derivative inquiries follow. First, which legal risks cannot be solved by ordinary electronic signatures alone? Second, which notarial functions add distinctive value without undermining digital efficiency, and how should they interact with platforms and electronic certification providers? Third, what regulatory model can harmonize consumer protection, electronic evidence, cybersecurity, privacy, and notarial authority? The objective is to formulate a doctrinal and policy model to guide regulation, notarial practice, platform governance, and dispute resolution.

The article proceeds in four analytical movements. It first explains the limits of signature-centered validity and the evidentiary consequences of fragmented regulation. It then develops the five-layer trust model and its doctrinal foundations. The third part identifies proportional risk indicators and an operational sequence for selective authentication. The final part examines implementation challenges, including evidence, privacy and data protection, vulnerable consumers, costs, cross-border

transactions, professional competence, and institutional coordination. This structure links the doctrinal argument directly to the regulatory design proposed in the article.

This study uses normative legal research because the problem concerns the coherence, interpretation, and reconstruction of legal norms governing electronic agreements, consumer protection, cyber law, privacy, evidence, and notarial authority. The research is doctrinal and prescriptive: it evaluates *ius constitutum* and formulates an *ius constituendum* model for selective notarial authentication. Legal materials are interpreted grammatically to identify the ordinary meaning and formal scope of relevant provisions, systematically to reconcile rules across contract, consumer, electronic-transaction, evidence, data-protection, and notarial regimes, and teleologically to assess those rules against legal certainty, fairness, preventive justice, and effective consumer protection. These interpretive methods prevent the proposed model from being treated as a purely technological design detached from the legal purposes of the institutions involved.

The statutory approach is used to analyse Indonesian legal materials, including the Civil Code, Law Number 8 of 1999 on Consumer Protection, Law Number 30 of 2004 as amended by Law Number 2 of 2014 on Notarial Office, Law Number 1 of 2024 on the second amendment to the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019 on Electronic System and Transaction Operation, and Government Regulation Number 80 of 2019 on Trading through Electronic Systems. These instruments are read together rather than separately because an electronic consumer agreement simultaneously involves contract validity, consumer rights, digital records, electronic signatures, platform obligations, and evidence.

The conceptual approach clarifies authenticity, authentication, informed consent, electronic evidence, consumer vulnerability, cyber notary, and preventive justice. The article distinguishes between three concepts that are often conflated. First, an electronic signature associates a person with electronic information. Second, electronic certification is a trust service that supports identity, integrity, and non-repudiation. Third, notarial authentication is a public-law function that connects legal counselling, verification, formalization, and evidentiary preservation. The distinction matters because consumer protection cannot be reduced to the existence of a signature, and notarial authenticity cannot be reduced to the technology used to sign a record.

The comparative approach is limited and functional rather than transplant-oriented. I selected international and comparative materials because they address one or more functions required by the proposed model: legal recognition and reliability of electronic communications, consumer fairness and redress, trusted digital identity, or electronic trust services. UNCITRAL instruments provide functional-equivalence, non-discrimination, reliability, accessibility, and technology-neutrality principles (UNCITRAL, 1996, 2001, 2005); OECD and United Nations consumer instruments provide transparency, fair-business-practice, education, and effective-redress principles (OECD, 2021; UNCTAD, 2016); and the eIDAS framework is used as a functional reference for trust services and digital identity governance rather than as a rule to be transplanted into Indonesian law (European Parliament & Council of the European Union, 2024). Secondary literature was selected to represent the intersecting fields of digital consumer fairness, electronic evidence, cyber-notarial authority, accessibility, platform liability, and cross-border consumer protection. The

comparison asks which functions are transferable as principles and which remain dependent on domestic notarial authority and procedural law.

The analysis followed five steps. First, it identified recurring legal risks involving identity, consent, disclosure, integrity, privacy, platform-controlled records, and access to evidence. Second, it mapped the legally distinctive functions of notaries and separated them from the functions of electronic certification providers, platforms, regulators, and courts. Third, it tested the relevant norms through grammatical, systematic, and teleological interpretation. Fourth, it compared the identified functions with international trust and consumer-protection principles. Fifth, it synthesized the recurring risk-function relationships into five layers—identity, consent, integrity, disclosure, and redress—and then tested the model against proportionality, evidentiary challenge, privacy, accessibility, and institutional feasibility. Because the study is normative, its conclusions are prescriptive; empirical pilots, cost studies, and user testing remain necessary before full-scale implementation (Masnun, Muh. Ali, Prasetio, Dicky Eko, 2025).

The analysis has two limitations. First, it does not claim that all electronic consumer agreements should be made by notarial deed. Such a position would be impractical, costly, and inconsistent with the ordinary logic of mass digital commerce. Second, the study does not provide a technical cybersecurity audit of particular platforms. Its focus is legal architecture: how notarial authentication fits within the broader governance of electronic agreements. The proposed model should therefore be read as a legal and institutional framework that still requires further empirical testing, technological design, and implementing regulation.

B. RESULT AND DISCUSSION

1. Electronic consumer agreements and the limits of signature-centered validity

The first finding is that electronic consumer agreements create a cluster of legal risks that a signature-centered understanding of cyber law does not adequately address. Electronic signatures help identify the signatory and show intention to be bound. Still, they do not automatically prove that the consumer received clear information, understood the terms, had a realistic opportunity to review the contract, or was protected from unfair clauses. The weakness is especially visible in clickwrap, browsewrap, app-based subscriptions, online financing, marketplace transactions, and cross-border e-commerce. In those transactions, the consumer's assent is usually generated inside an interface designed and controlled by the business actor or platform. The trader also often stores the evidentiary record, which means the consumer may not have the full contract history when a dispute arises.

Consumer law and cyber law therefore begin from different normative anxieties. Consumer law asks whether the consumer has been treated fairly, informed properly, and protected from abusive terms. Cyber law asks whether the electronic record is reliable, secure, and legally recognized. A digital contract may satisfy the cyber-law test of electronic validity while still failing the consumer-law test of fairness. This is why a bridge is needed. Notarial authentication can provide that bridge when it is directed not only toward the final signature but toward the process of contract formation. The notary can verify whether the consumer received essential information,

whether the trader's identity is clear, whether the terms are stable at the time of agreement, and whether the evidence can be retrieved independently of the platform.

The Indonesian framework already contains parts of this bridge but has not yet assembled them into a coherent model. Law Number 8 of 1999 recognizes consumer protection as a legal regime concerned with rights, obligations, information, safety, and fairness (Republic of Indonesia, 1999). Government Regulation Number 80 of 2019 specifically governs trading through electronic systems and reflects the need to regulate the architecture of online trade (Republic of Indonesia, 2019b). Electronic transaction law recognizes electronic information and electronic documents as part of legal transactions. In contrast, notarial law preserves the authentic deed as a written evidentiary instrument made by or before a public official. Research in Jurnal Suara Hukum confirms that electronic contractual validity and consumer rights in e-commerce cannot be separated from questions of data security, contractual transparency, and legal responsibility (Zamzam et al., 2023). The problem is therefore not the absence of norms, but fragmentation. Each regime has its own object, vocabulary, and institutional logic.

Fragmentation has consequences in litigation. When a consumer challenges an electronic agreement, the dispute may turn on whether the electronic record is complete, whether the consumer actually accepted the clause relied upon by the trader, whether a later version of terms replaced an earlier version, whether the identity of the seller can be traced, and whether the data stored by the platform is admissible and reliable. Without independent authentication, the consumer may have to rely on the very party being challenged. The business actor controls logs, timestamps, terms-and-conditions repositories, customer-service records, and sometimes payment metadata.

Notarial authentication can reduce this asymmetry by creating an independent evidentiary layer that preserves the relevant contractual facts at the moment of formation.

The second finding is that notarial authentication should be understood as a continuum of legal functions. At the lowest level, the notary may certify the date, identity, or conformity of a copy of an electronic record. At a higher level, the notary may supervise the signing process, verify the parties' legal capacity, and preserve the agreement's final version. At the highest level, the notary may formalize the agreement as an authentic deed when the law requires or permits such form. These levels should not be confused. The fact that a notary authenticates an electronic agreement does not necessarily mean that the electronic agreement becomes an authentic deed in the traditional sense. The legal effect depends on the form, the statutory authority invoked, and the procedural safeguards followed.

This distinction is essential for consumer transactions. Many consumer agreements do not require authentic deeds. In these cases, notarial authentication can provide stronger evidence and preventive legal counselling. Some transactions, however, may involve objects or obligations that require formal notarial involvement, such as certain guarantees, security arrangements, corporate-related consumer investments, or long-term property-linked contracts. In these cases, the challenge is deeper because the electronic agreement may collide with formal deed requirements. The regulatory solution should clarify which notarial acts can be performed electronically, which must remain physically executed, and which can be hybridized through secure audiovisual appearance, qualified electronic signatures, digital identity verification, and encrypted document custody.

Table 1. Legal risks and notarial authentication responses in electronic consumer agreements

Risk in electronic consumer agreements	Why ordinary electronic signatures are insufficient	Notarial authentication response
Identity uncertainty	Credentials may be shared, stolen, delegated, or created under a false identity.	Verify legal identity capacity, and link between person and credential.
Uninformed consent	A click may prove assent but not meaningful understanding of essential terms.	Record disclosure review warnings for risk clauses and confirmation of comprehension.
Dynamic contract terms	Platforms may update terms and make it difficult to prove which version applied.	Hash, timestamp, archive and issue authenticated consumer copy.
Evidence asymmetry	Trader or platform controls logs, data, and contract history.	Create independent evidentiary file accessible for dispute resolution.
Cross-border enforcement	Foreign law, foreign forum, and platform terms may weaken local consumer remedies.	Certify party identity governing-law notice dispute clause, and consumer acknowledgement.

Source: Author's synthesis based on consumer protection, cyber law, and notarial law principles.

Table 1 demonstrates that the legal function of notarial authentication is not limited to attaching authority to the final signature. The most serious risks arise before and after signature: before signature, when the consumer receives information and decides whether to agree; after signature, when the consumer must prove the agreement and challenge misconduct. A notarial protocol that ignores these phases would reproduce the weakness of signature-centered validity. A protocol that covers identity, consent, content integrity, disclosure, and redress can instead transform digital contracting into a more accountable legal process.

2. Notarial authentication as a layered trust infrastructure

The proposed bridge begins with identity. In ordinary e-commerce, identity is often reduced to account credentials, mobile numbers, email addresses, payment cards,

or one-time passwords. These indicators may be sufficient for low-value purchases, but they are fragile for high-risk consumer agreements. Identity fraud, account takeover, synthetic identity, and misuse of digital credentials can create disputes in which the consumer denies having entered the contract. A notarial authentication protocol would require identity verification based on government identity documents, electronic certificates, biometric or liveness checks where lawful, and confirmation that the person controlling the digital credential is the person assuming the legal obligation. The notary would not replace electronic certification providers, but would add a legal-verification layer that connects technical identity to legal capacity.

The second layer is consent. Consent in electronic transactions is often evidenced by a click, checkbox, digital signature, or typed name, but formal assent does not resolve whether consent was legally meaningful. Contract doctrine concerning mistake, fraud or misrepresentation, coercion, and undue influence remains relevant when interface design obscures material facts, accelerates acceptance, exploits dependency, or bundles unrelated permissions. The notary's function is not to guarantee that every contractual judgment is wise, but to reduce avoidable defects in formation by verifying that essential information was available, highlighting unusually burdensome clauses, and recording a deliberate final approval. The protocol must also examine lawful cause and object: authentication cannot cure an unlawful obligation or transform a prohibited clause into a valid one. Accordingly, the notarial statement should certify the process actually performed, not the substantive legality of every future performance dispute.

The third layer is content integrity. A recurring problem in electronic agreements is proving which version of the terms applied at the moment of acceptance. Traders

may update terms, platforms may store dynamic documents, and consumers may have only screenshots or confirmation emails. A notarial protocol could require hashing the final agreement, timestamping, secure archiving, and generating a consumer-accessible authenticated copy. Hash values and timestamps should be treated not as decorative technical features but as evidentiary anchors. They ensure that the agreement presented in dispute resolution is the same agreement that was authenticated at formation.

The fourth layer is disclosure. Consumer protection requires more than information availability. It requires information to be timely, clear, accessible, and relevant. In digital contexts, disclosure should include the trader's identity and address, product or service characteristics, total price, taxes, delivery terms, complaint channels, cancellation rights where applicable, warranty information, data-processing implications, and dispute-resolution mechanisms. Notarial authentication can certify that the disclosure package was presented and attached to the agreement. This can be particularly important in cross-border consumer transactions, where consumers may face foreign sellers, foreign platforms, foreign currencies, foreign dispute forums, and unfamiliar legal terms.

The fifth layer is redress. Consumer protection fails when rights exist on paper but cannot be enforced. Electronic agreements must therefore be designed with evidence portability. The consumer should be able to obtain an authenticated copy, transaction log, proof of disclosure, proof of consent, and contact information for complaint handling. The notary can serve as custodian of a sealed evidentiary record and, where appropriate, certify extracts for use before courts, consumer dispute settlement bodies, arbitration institutions, or platform complaint mechanisms. This

function resonates with the preventive character of notarial practice: the notary reduces future conflict by structuring reliable evidence at the beginning of the transaction.

These five layers show why notarial authentication is different from ordinary electronic signatures. A signature answers the question "who approved this record?" Notarial authentication answers a broader set of questions: who the parties were, what exactly was approved, when it was approved, under what information conditions it was approved, how the record was preserved, and how the consumer can prove it later. This broader evidentiary frame is the article's principal finding. It allows notarial law to contribute to cyber law without claiming monopoly over all digital transactions.

Table 2. Five-layer model of notarial consumer authentication

Layer	Core Legal Question	Minimum Notarial Protocol
Identity	Who is legally bound by the agreement?	Identity verification, capacity check, and a link to an electronic certificate or verified credential.
Consent	Was agreement voluntary and meaningful?	Reading or explaining essential terms, recording warnings for risk clauses, documenting final approval.
Integrity	Is the record the same as the agreed text?	Hash value, timestamp, sealed archive, version control, authenticated copy.
Disclosure	Did the consumer receive essential information?	Attach disclosure package and certify presentation before signature.
Redress	Can the consumer enforce rights later?	Evidence custody, copy access, certified extracts, complaint-path documentation.

Source: Author's proposed framework.

Table 2 summarizes the proposed five-layer model. The model is intentionally modular. For ordinary transactions, only minimal layers may be needed. For complex

or high-risk transactions, all layers should be activated. This modularity allows law and practice to avoid an all-or-nothing choice between complete informality and traditional paper formalism. It also allows notaries, platforms, and regulators to develop risk-based procedures that are sensitive to the value and consequences of the transaction.

3. Bridging consumer protection and cyber law through proportional authentication

The third finding concerns proportionality. Notarial authentication should not be mandatory for every electronic consumer agreement because universal notarization would burden consumers, slow commerce, and create unnecessary formality. Instead, an objective risk matrix should trigger selective authentication. Relevant indicators include transaction value relative to ordinary consumer purchases, long duration, deferred or recurring payment, embedded financing, cross-border seller identity, sensitive or large-scale personal-data processing, difficult-to-reverse digital rights, arbitration or foreign-forum clauses, unilateral-amendment clauses, waivers or limitations of consumer rights, and demonstrable consumer vulnerability. No single monetary threshold is universally sufficient; regulators should combine quantitative thresholds with qualitative consequences. Multiple indicators, or one indicator carrying exceptional legal consequences, should trigger the full five-layer protocol, while lower-risk transactions should use lighter forms of verification.

A proportional model also protects the notarial profession from technological overreach. If notaries are asked merely to click a digital certificate or witness a screen without legal review, the profession risks becoming a decorative add-on to platform design. Conversely, if notaries insist on paper-only authenticity, they risk irrelevance

in digital markets. The proper position is functional modernization. The notary should retain the essence of office independence, impartiality, legal counselling, formality, document custody, and evidentiary reliability, while adapting the medium through regulated technology. This requires secure platforms, clear protocols, professional training, and oversight by the notarial supervisory structure.

The fourth finding is that cyber law must be read through the lens of consumer protection values. The principle of technology neutrality should not become value neutrality (Masnun et al., 2025). A legal system may recognize many technologies as capable of producing electronic signatures, but consumer transactions require additional scrutiny because consumers rarely choose the technology. The trader or platform chooses the authentication method, interface, storage architecture, and dispute process. Therefore, evaluate reliability from the consumer's perspective. A system that is technically secure for the trader may still be legally inadequate if it prevents the consumer from accessing evidence, understanding obligations, or challenging unfair terms.

The comparative materials support this value-sensitive approach. UNCITRAL instruments emphasize functional equivalence and non-discrimination against electronic communications, but they also link legal effect to reliability, intention, and accessibility (UNCITRAL, 1996, 2001, 2005). OECD and UN consumer-protection instruments emphasize fair business practices, transparency, effective redress, and consumer education in e-commerce (OECD, 2021; UNCTAD, 2016). European digital identity reforms show the movement toward trusted digital identity and trust services as infrastructure for online transactions (European Parliament & Council of the European Union, 2024). At the regional level, analysis in *Jurnal Suara Hukum* of the

ASEAN Agreement on E-Commerce shows that cross-border digital commerce requires closer alignment between electronic-contract rules, legal certainty, security, and national regulatory frameworks (Wilbert et al., 2024). These developments do not produce a single universal model, but they confirm that digital contracting must combine technological recognition with institutional trust and user protection.

In Indonesian law, this means modernizing notarial authentication should be coordinated with consumer protection agencies, electronic system regulators, data-protection authorities, trade authorities, and courts. A notarially authenticated electronic consumer agreement should not simply be a private document stored in a notary's computer. It should satisfy minimum standards of system security, auditability, access control, consumer copy delivery, data retention, and confidentiality. The notary should also be protected from being turned into a platform vendor or data processor without clear responsibilities. Regulatory design must define the boundaries of the notary's liability, the duties of electronic certification providers, the obligations of traders, and consumers' rights to obtain authenticated records.

The fifth finding is that notarial authentication can operate as a form of preventive consumer justice. Preventive justice means structuring legal relations to avoid disputes or reduce their intensity before they arise. In electronic consumer agreements, preventive justice is achieved when the consumer understands essential terms, the trader cannot easily manipulate evidence, and the platform must maintain reliable transaction records. The notary's independent role changes the incentive structure. Traders know that contractual disclosures and consent mechanisms may be reviewed. Consumers know that an authenticated evidentiary file exists. Courts and

dispute institutions receive a clearer record. The overall result is not merely stronger evidence but better contracting behaviour.

4. Regulatory implications for notarial practice and digital consumer justice

The findings lead to a regulatory model built on five principles. The first principle is differentiated formality. The law should distinguish ordinary electronic consumer contracts, electronically authenticated contracts, and electronic authentic deeds. Ordinary contracts may rely on standard electronic signatures or platform records. Authenticated contracts require an independent notarial protocol for identity, consent, disclosure, integrity, and custody. Electronic authentic deeds, if permitted, must comply with a higher statutory form that clearly regulates appearance, reading, signing, storage, minutes, copies, and supervisory control. This differentiation prevents both excessive formalism and excessive informality.

The second principle is consumer-centered authentication. Authentication should not be designed solely to protect traders against repudiation. It should also protect consumers against hidden terms, identity misuse, inaccessible evidence, and unfair dispute clauses. The protocol should require plain-language summaries of essential terms, prominent disclosure of risk clauses, and confirmation that the consumer can download or receive the authenticated record. Where the consumer is vulnerable because of disability, language, age, digital literacy, or financial pressure, additional safeguards may be justified. This orientation aligns with Jurnal Suara Hukum scholarship, which treats consumer rights as part of a broader justice framework and highlights the need to strengthen transparency, privacy protection, and access to effective remedies in digital transactions (Kadir et al., 2024). Waddington's

work on accessible pre-contractual information is also instructive because it shows that consumer protection must consider how information is actually received, not merely whether it exists (Waddington, 2022).

The third principle is technological neutrality with minimum reliability. Law should not freeze one technology as the only valid method. However, neutrality must be paired with minimum standards. A notarial authentication platform should support secure identity verification, tamper-evident records, encryption, strong access control, trusted timestamps, audit logs, retention periods, and data-backup mechanisms. It should also provide interoperability with recognized electronic certificates where applicable. The notary's role should remain legal and institutional, while technical providers should be subject to certification, security audits, and liability rules.

The fourth principle is evidence portability and contestability. The authenticated agreement must remain usable beyond the platform where it was created. Consumers should receive a complete copy with metadata that proves the date, content, parties, disclosure, signature, and scope of the notarial act. The notary should maintain a secure archive and be able to certify copies or extracts. Notarial authentication should create strengthened written electronic evidence, not an irrebuttable presumption. A court must remain able to examine fraud, coercion, identity compromise, unlawful cause, system failure, alteration, lack of authority, or non-compliance with mandatory notarial procedure. The probative consequence should therefore depend on what the notary actually verified: identity certification supports attribution; timestamp and hash support integrity; recorded disclosure supports proof of presentation; and custody supports continuity of evidence. This differentiated evidentiary effect preserves procedural fairness while reducing disputes about provenance and version history.

The fifth principle is institutional coordination. Notarial authentication will fail if notarial law alone regulates it. It requires coordination among the Ministry responsible for notarial supervision, regulators of electronic systems, trade authorities, consumer protection bodies, courts, electronic certification providers, and professional associations. Coordination should cover technical standards, training, complaint channels, disciplinary mechanisms, data protection, cross-border evidence, and consumer education. The notarial profession should not be left alone to improvise digital procedures, and platforms should not be allowed to define legal authenticity unilaterally.

Based on these principles, this article proposes a five-layer model, the Notarial Consumer Authentication Framework. The framework begins before signature and continues after contract formation. Before signature, the notary verifies identity, capacity, and disclosure. During signature, the notary records consent, timestamps the agreement, and certifies the final text. After signature, the notary preserves the record, issues authenticated copies, and supports evidentiary retrieval. The model is flexible enough to apply to remote transactions, hybrid transactions, and cross-border consumer agreements, provided that implementing regulations clarify procedures and liability.

Table 3. Policy Directions for Regulating Notarial Authentication of Electronic Consumer Agreements

Regulatory issue	Recommended Rule	Expected legal effect
Scope of use	Apply notarial authentication to high-risk electronic consumer agreements.	Prevents excessive formalism while targeting vulnerable transactions.
Remote appearance	Permit secure audiovisual appearance only under statutory safeguards.	Maintains legal counselling and identity control in digital settings.

Electronic evidence	Recognize authenticated records as strong written electronic evidence subject to challenge.	Improves certainty without eliminating procedural fairness.
Consumer access	Require immediate delivery of authenticated copies and metadata.	Reduces evidence asymmetry and improves access to redress.
Institutional oversight	Coordinate notarial, trade, cyber, data protection, and consumer authorities.	Prevents fragmented governance and inconsistent enforcement.

Source: Author's normative recommendations.

Table 3 translates the doctrinal findings into regulatory directions. The key point is coordination. A notarial-authentication regime will not be credible if it is developed solely as a professional internal practice, because electronic consumer agreements also involve platform governance, cybersecurity, trade regulation, data protection, and consumer redress. Conversely, a cyber-law regime will remain incomplete if it treats authentication as purely technical and ignores the preventive function of legal professionals. The bridge must therefore be institutional as well as doctrinal.

5. Operationalization of the proposed framework

Operationalizing the model requires a procedural sequence that notaries, platforms, and consumers can understand. The first stage is pre-authentication screening. At this stage, the notary or authorized notarial platform determines whether the transaction falls under a high-risk electronic consumer agreement. The screening should not be based only on nominal value. A low-price transaction may still carry high consequences if it involves recurring payments, long-term data processing, digital identity, health information, education financing, property access, insurance claims, or the transfer of rights that are difficult to reverse. The screening stage therefore functions as the gateway that decides whether the legal risk justifies the cost of authentication.

The second stage is trader verification. Consumer protection in digital markets is often undermined not because consumers cannot sign electronically, but because they cannot identify the real trader. Marketplace sellers, dropshippers, affiliates, and offshore service providers may appear through platform profiles that conceal their legal personality, address, licensing status, or complaint-handling capacity. A notarial authentication mechanism should require the trader to disclose its legal name, registration number where applicable, address, authorized representative, contact channel, and relationship with the platform. This information should be attached to the authenticated record. If the trader acts through an agent, the notary should verify the agent's authority to bind the trader.

The third stage is consumer verification and legal-capacity assessment. Digital platforms often treat account access as sufficient proof of contracting capacity. Notarial practice cannot stop there. The notary should confirm that the consumer is the person entering the agreement, is legally competent, and is not obviously entering it under coercion, deception, or identity misuse. In remote settings, this may require secure audiovisual interaction, identity-document verification, comparison with electronic certificates, and additional safeguards where the transaction involves elderly consumers, minors, disabled consumers, or consumers who show signs of misunderstanding. These safeguards must be designed with data minimization so that authentication does not become excessive surveillance.

The fourth stage is disclosure certification. The notary should not rewrite commercial terms for the parties, but the notary can certify that essential information was presented in a stable and accessible form. This includes the main characteristics of goods or services, total price, payment schedule, delivery or performance time,

cancellation rights, warranty terms, data-processing consequences, complaint procedure, and dispute forum. Highlight clauses that restrict consumer rights separately. Such clauses include limitation of liability, unilateral amendment, automatic renewal, penalties, acceleration, mandatory arbitration, foreign-law selection, foreign-court selection, waiver of class action, and broad personal-data permissions. The consumer's acknowledgement of these clauses should be recorded more deliberately than a single bundled click.

The fifth stage is authenticated execution. The final agreement should be locked before signature so the signed document matches the stored document. The authentication system should generate a timestamp, hash value, signer identity record, certificate reference where relevant, and notarial authentication statement. The notary should record whether the agreement was read, explained, or summarized; whether the parties appeared physically, remotely, or through a hybrid method; and whether any technical interruption occurred. The authentication statement should be concise but legally meaningful. It should identify the scope of the notary's certification so that later disputes do not treat the notary as guarantor of product quality or business performance.

The sixth stage is custody and access. Digital evidence is fragile when it depends on private servers that may change, disappear, or refuse access. The notary should preserve the authenticated record in encrypted storage with retention periods consistent with notarial archive rules and data-protection duties. The consumer should receive an authenticated copy immediately, preferably in a format that can be independently verified. Where the consumer loses access, a replacement copy or certified extract should be obtainable through a clear procedure. This custody function is central to the

bridge between cyber law and consumer protection because it converts technical traces into legally usable evidence.

The seventh stage is complaint support. Notarial authentication should not turn the notary into a consumer dispute judge, but it should facilitate redress. When a dispute arises, the notary may certify copies, confirm the metadata of the authenticated agreement, and explain the scope of the authentication act. Consumer dispute bodies and courts can then examine the substantive claim using a more reliable evidentiary base. This reduces the time spent arguing about whether the agreement exists, which version applies, who signed it, and what disclosures were presented. The dispute can focus on the substantive issues: breach, unfairness, defect, non-delivery, misrepresentation, or violation of consumer rights.

The model also has implications for private international law. Electronic consumer agreements frequently contain choice-of-law and choice-of-forum clauses. In a cross-border transaction, such clauses may deprive consumers of accessible remedies if they are hidden in standard terms or designed to select distant fora. The ASEAN e-commerce framework also demonstrates that cross-border electronic contracting raises linked questions of legal certainty, security, sovereignty, and harmonization of contract rules (Wilbert et al., 2024). Notarial authentication cannot solve all jurisdictional issues, but it can require that these clauses be specifically disclosed and separately acknowledged. The notary can certify that the consumer was informed that the dispute may be governed by foreign law or resolved before a foreign court or arbitral institution. This does not necessarily validate an unfair clause. Still, it creates a record that helps courts decide whether the clause was transparent, reasonable, and consistent with mandatory consumer protection norms.

A further implication concerns data protection. Electronic consumer agreements often combine contract formation with consent to process personal data. This creates a risk of consent bundling, where the consumer cannot separate contractual consent from data-processing permission. A notarial authentication protocol should identify data-sensitive clauses and require clearer separation between contractual obligations and data permissions. The notary does not become a data-protection authority, but the notarial record can show whether the consumer received notice of data collection, purpose, retention, sharing, and withdrawal mechanisms. In high-risk transactions, this documentation may prevent later disputes over whether data-related consent was freely and specifically given.

Finally, the model requires professional competence. Notaries who authenticate electronic agreements must understand not only civil law and deed formalities but also electronic signatures, digital identity, cybersecurity basics, platform contracting, consumer vulnerability, and data protection. Professional training should therefore include digital evidence, secure communication, remote appearance ethics, data minimization, electronic archive management, and recognition of manipulative interface design. Without this competence, cyber notary will become a slogan rather than a reliable legal practice. With it, the notarial profession can become a credible institutional guardian of trust in digital private law.

A human-rights perspective further explains why the model must remain selective and consumer-centered. Digital contracting can affect privacy and informational autonomy when contractual assent is bundled with broad data-processing permissions; equality when elderly consumers, persons with disabilities, persons with limited digital literacy, or consumers under financial pressure cannot use

the same interface on equal terms; and access to justice when the trader controls the only usable evidence. Recent *Jurnal Suara Hukum* scholarship on digital contract transformation similarly argues that legal certainty in technologically mediated contracting should be integrated with a human-rights-based approach rather than treated as a purely technical validity question (Priyono et al., 2026). Notarial authentication can function as an institutional safeguard for autonomy and dignity only if it improves understanding and contestability rather than adding coercive formality. Reasonable accommodation, accessible explanations, additional time, assisted communication, and alternative authentication channels should therefore be available where needed, without lowering the consumer's legal agency.

Privacy and data protection also constrain authentication architecture. Identity verification, audiovisual appearance, biometric or liveness checks, transaction logs, and long-term evidence custody may create new privacy risks if they collect more information than necessary. Comparative research published in *Jurnal Suara Hukum* underscores that privacy and personal-data protection require coherent safeguards, legal harmonization, and clear limits on data use (Tsamara, 2021), while e-commerce research in the same journal links electronic contractual relations to legal responsibility for personal-data breaches (Zamzam et al., 2023). The protocol should therefore apply purpose limitation, data minimization, role-based access, encryption, retention limits, auditable disclosure, and clear allocation of responsibility among the notary, platform, and technical provider. Contractual consent and data-processing permission should be separated where the law requires distinct legal bases. The notary should document that required notices were presented but should not become a general data-protection authority or an unrestricted repository of consumer data.

Implementation costs should be assessed on a proportionality basis rather than through speculative fixed prices. The principal costs arise from professional time, identity verification, secure audiovisual infrastructure, trusted timestamps, hashing, encrypted custody, and later copy retrieval. A high-value financed vehicle purchase or long-term cross-border service may justify the full protocol because the expected cost of identity fraud, unfair terms, or evidentiary failure is substantial. By contrast, an ordinary low-value subscription should normally remain outside mandatory notarial authentication unless recurring payment, sensitive data, or unusually restrictive clauses materially increase risk. Regulators should test fee caps, digital workflow time, consumer accessibility, and platform integration through pilot programs before setting mandatory thresholds. This risk-based cost-benefit approach avoids inventing unsupported price estimates while answering the practical concern that authentication must not become a barrier to e-commerce.

C. CONCLUSION

This article concludes that selective notarial authentication can strengthen electronic consumer agreements when it is reconstructed beyond signature validation and confined to transactions in which vulnerability and evidentiary risk justify additional formality. The five-layer model—identity verification, meaningful-consent confirmation, content-integrity preservation, disclosure certification, and redress-oriented evidence custody—connects consumer fairness with cyber-law reliability and the preventive function of notarial practice. Its legal value is differentiated: authentication can strengthen attribution, integrity, disclosure, and evidence custody

without automatically converting every electronic agreement into an authentic deed or preventing judicial challenge.

Regulatory reform should proceed in a clear order of priority. First, the legal status and evidentiary consequences of notarially authenticated electronic agreements should be distinguished from both ordinary electronic contracts and electronic authentic deeds. Second, implementing standards should govern risk-based scope, remote appearance, identity verification, informed-consent records, timestamps, hashing, secure custody, privacy and data minimization, accessibility, consumer copies, and procedures for evidentiary challenge. Third, professional training should equip notaries to address digital evidence, consumer vulnerability, manipulative interface design, cybersecurity basics, and data protection. Fourth, notarial, trade, electronic-system, data-protection, consumer-protection, certification, and judicial institutions should coordinate technical standards, supervision, complaints, and cross-border evidence. These priorities provide a practical pathway to use the five-layer model as a template for preventive digital consumer justice while preserving efficient, low-risk e-commerce.

Future research should test the proposed framework empirically by examining consumer disputes involving electronic agreements, interviewing notaries and electronic certification providers, and evaluating platform practices in preserving contract evidence. Comparative research may also study jurisdictions that have adopted remote online notarization, qualified trust services, or digital identity wallets. The deeper challenge is not technological feasibility but institutional legitimacy. Digital contracting needs trust, and code alone cannot produce it. It requires legal institutions that can make digital records understandable, reliable, contestable, and fair.

REFERENCES

- Chen, J. (2023). Consumer protection in digital markets and platform-based transactions. *Journal of Consumer Policy*, 46(1), 1-22.
- Dewi, R. S. (2021). Cyber notary and the transformation of notarial authority in Indonesia. *Indonesian Journal of Law and Society*, 2(2), 145-166.
- Durovic, M., & Poon, J. (2023). Digital fairness and consumer protection in platform commerce. *European Review of Private Law*, 31(2), 215-240.
- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
- Howells, G. (2020). Protecting consumer protection values in the fourth industrial revolution. *Journal of Consumer Policy*, 43(1), 1-17.
- Kadir, M. Y. A., Arifin, M., Disantara, F. P., Thuong, M. T. H., & Nutako, B. S. M. (2024). The reform of consumer protection law: Comparison of Indonesia, Vietnam, and Ghana. *Jurnal Suara Hukum*, 6(2), 255-278.
<https://doi.org/10.26740/jsh.v6n2.p255-278>
- Masnun, Muh. Ali, Prasetio, Dicky Eko, M. (2025). Reconstruction of the Normative Legal Research Paradigm in Responding to Global Challenges: An Epistemological Analysis. *Novum: Jurnal Hukum*, 12(3), 372–384.
<https://doi.org/https://doi.org/10.2674/novum.v12i03.74364>
- Masnun, M. A., Prasetio, D. E., Ikram, D., & P, P. A. (2025). Legal Reform of Legal

- Profession Amidst the Development of Artificial Intelligence in Indonesia: The Perspective of Mesu Budi's Philosophy of Law. *Novum: Jurnal Hukum*, 12(2), 277–287. <https://doi.org/https://doi.org/10.2674/novum.v12i02.72355>
- Meskić, Z. (2022). Consumer protection and private international law in digital markets. *Journal of Private International Law*, 18(2), 275-299.
- Muh. Ali Masnun, Dicky Eko Prasetyo, Mohd Badrol Awang, E. S. (2024). Reconstructing Indonesia's Trademark Registration System through the Lens of General Principles of Good Governance to Realize Substantive Justice. *Journal of Law and Legal Reform*, 5(3), 891–912.
- OECD. (2021). Recommendation of the Council on Consumer Protection in E-Commerce. Paris: OECD Publishing.
- Prabhawisnu, I. G. A. (2023). Electronic deeds and digital signatures in cyber notary practice. *Jurnal Hukum dan Kenotariatan*, 7(1), 33-52.
- Prasetyo, D. E., Masnun, M. A., Disantara, F. P., & Noviyanti, N. (2025). The Construction Of The Lex Sportiva Principle In Indonesia's Sports Law: Implications And Future Arrangements. *UUM Journal of Legal Studies*, 16(2), 58–69. <https://doi.org/10.32890/uumjls2025.16.2.4>
- Priyono, E. A., Akinrinde, O. O., Al Fithri, M. N., & Azhar, M. (2026). Digital transformation of contract law: Legal certainty and human rights protection in AI-based contracts. *Jurnal Suara Hukum*, 8(1), 132-166. <https://doi.org/10.26740/jsh.v8n1.p132-166>

- Republic of Indonesia. (1999). Law Number 8 of 1999 on Consumer Protection.
- Republic of Indonesia. (2014). Law Number 2 of 2014 concerning Amendment to Law Number 30 of 2004 on Notarial Office.
- Republic of Indonesia. (2019a). Government Regulation Number 71 of 2019 on Electronic System and Transaction Operation.
- Republic of Indonesia. (2019b). Government Regulation Number 80 of 2019 on Trading through Electronic Systems.
- Republic of Indonesia. (2024). Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law.
- Sulistiyowati, Eny, Muh. Ali Masnun, D. E. P. (2025). Arrangements for online food delivery service drivers to achieve food safety. *IOP Conf. Series: Earth and Environmental Science*, 1454(1), 1–7.
- Tsamara, N. (2021). Perbandingan aturan perlindungan privasi atas data pribadi antara Indonesia dengan beberapa negara. *Jurnal Suara Hukum*, 3(1), 53-84.
<https://doi.org/10.26740/jsh.v3n1.p53-84>
- UNCITRAL. (1996). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment. New York: United Nations.
- UNCITRAL. (2001). UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. New York: United Nations.

- UNCITRAL. (2005). United Nations Convention on the Use of Electronic Communications in International Contracts. New York: United Nations.
- UNCTAD. (2016). United Nations Guidelines for Consumer Protection. Geneva: United Nations.
- Waddington, L. (2022). Accessible pre-contractual information and consumer protection in digital environments. *European Consumer and Market Law Journal*, 11(3), 98-107.
- Wibowo, A. (2024). Platform liability and consumer protection in Indonesia's digital economy. *Jurnal Hukum Ius Quia Iustum*, 31(1), 1-25.
- Wilbert, W., Siregar, M., Sukarja, D., & Natcha, N. (2024). Legal analysis of the implications of the ASEAN Agreement on E-Commerce for electronic business contracts in Indonesia. *Jurnal Suara Hukum*, 6(1), 48-67.
<https://doi.org/10.26740/jsh.v6n1.p48-67>
- Zamzam, M. I. M., Arsyada, R. M., & Al'Azza, N. E. A. (2023). Keabsahan hubungan kontraktual secara elektronik dalam e-commerce dan pertanggungjawaban hukum atas kebocoran data pribadi pengguna. *Jurnal Suara Hukum*, 5(2), 130-148. <https://doi.org/10.26740/jsh.v5n2.p130-148>