

Time-Bound Tiered Liability Doctrine in Indonesia’s QRIS Ecosystem: A Proportional Justice Approach to Legal Protection

Elfina Yosepha¹ Reka Dewantara² Patricia Audrey Ruslijanto³ Mohammad Azam⁴ Maminiaina Heritiana Sedera⁵

^{1,2,3v}Faculty of Law, Brawijaya University, Jl. MT. Haryono No.169, Ketawanggede, Malang, Indonesia

⁴Al Iraquia University Baghdad

⁵ISCAM Business and Law School, Madagascar

elfinayosephaa@gmail.com¹, rainerfh@ub.ac.id², patricia@ub.ac.id³ aliraqia.edu.iq⁴, fenitra.rakotoarisoa@gmail.com⁵

Article Info

Received: 2026-05-10

Revised: 2026-10-16

Accepted: 2026-10-21

Keywords:

Consumer Protection; Legal Liability; QRIS; Time-Bound Tiered Liability; Unauthorized Transactions.

Abstract

The expansion of the Quick Response Code Indonesian Standard (QRIS) has intensified the need for clear rules on liability and reimbursement for unauthorized transactions. This study examines Indonesia’s regulatory framework and formulates the Time-Bound Tiered Liability Doctrine as a policy reform proposal. Using normative legal research through statutory, conceptual, and comparative approaches, it analyses Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 1 of 2024; Law No. 8 of 1999 on Consumer Protection; Government Regulation No. 71 of 2019; Bank Indonesia Regulations Nos. 6 of 2026 and 10 of 2025; and Bank Indonesia Board of Governors Member Regulation No. 32 of 2026. Comparative analysis draws on United States Regulation E and Directive (EU) 2015/2366. The study finds that Indonesian law recognises provider liability, shared responsibility, provider evidentiary burdens, and complaint-handling periods. However, it lacks a dedicated regime connecting notification timing with graduated consumer liability, preventable additional loss, and substantive reimbursement deadlines for unauthorized QRIS transactions. Drawing on comparative principles of timely notification, causation, and reimbursement, the study proposes four reporting tiers with thresholds of 24 hours, three business days, seven calendar days, and 60 days. These thresholds are normative recommendations informed by proportionality and loss mitigation, with the 24-hour threshold reflecting QRIS’s real-time operation and continuous reporting channels. Prompt reporting should attract full reimbursement, subject to proven fraud or intentional misconduct, while later tiers permit consumer liability of up to 10%, 25%, and 50% of additional losses the provider proves could have been prevented. The model also requires provisional reimbursement and reasonable exceptions for justified reporting delays. Its novelty lies in operationalising existing responsibility rules through a model integrating notification time, fault, causation, and loss prevention. Its legal contribution is a structured distinction between initial loss and preventable additional loss, coupled with enforceable reimbursement obligations. Incorporation into a Bank Indonesia Regulation, supported by implementing rules and provider procedures, would promote legal certainty, proportional justice, and consistent consumer redress.

I. Introduction

The rapid institutionalisation of the Quick Response Code Indonesian Standard (QRIS) has transformed it from a technical payment standard into a central infrastructure of Indonesia's retail economy. QRIS connects bank accounts, electronic money, mobile-banking applications, digital wallets, payment service providers, merchants, switching institutions, and supporting entities through a common interoperable channel. Its expansion has been exceptional. As of October 2023, QRIS had reached 43.44 million users and 29.63 million merchants, the majority of which were micro, small, and medium-sized enterprises. Additionally, the transaction value grew by 186.08% year-on-year (Subihana Putri et al., 2025). QRIS is therefore no longer a peripheral financial-technology product, it is mass-market payment infrastructure whose legal reliability directly affects household liquidity, merchant turnover, public confidence, and the stability of Indonesia's digital economy.

Importance of QRIS grows in proportion to its scale. A system that transmits payments instantaneously may also transmit losses instantaneously. Unauthorized transactions may arise from stolen credentials, account takeover, phishing, malware, social engineering, SIM-card compromise, device theft, falsified merchant QR codes, data manipulation, defective authentication, or failures in fraud-monitoring systems. A consumer may discover that funds have been debited even though no valid consent was ever given (Tara & Sudiro, 2023).

The consumer must then confront a technologically complex payment chain while having limited access to system logs, device-binding records, authentication data, merchant-acquiring information, and switching records. The institutions controlling the evidence are ordinarily the same institutions whose responsibility is disputed. This evidentiary asymmetry places consumers in a structurally weaker position and makes risk allocation a matter of substantive justice rather than

contractual administration (Wicaksono et al., 2026).

Indonesia does not operate in a complete regulatory vacuum concerning unauthorized transactions within the QRIS ecosystem. Article 15 paragraphs (1) and (2) of Law Number 11 of 2008 on Electronic Information and Transactions, as last amended by Law Number 1 of 2024, requires every Electronic System Provider to operate its system reliably and securely and to assume responsibility for its proper operation, subject to the exception under Article 15 paragraph (3) where force majeure or user fault or negligence is proven. Article 21 further allocates responsibility for transactions conducted through Electronic Agents, placing liability upon the operator where losses result from direct third-party interference with the electronic system, while attributing responsibility to the user where the failure is caused by the user's negligence. Although these provisions may apply to mobile-banking applications, electronic wallets, and other automated QRIS payment facilities, they do not distinguish ordinary negligence from gross negligence or prescribe a maximum level of consumer liability (Ramah et al., 2024). The Consumer Protection Law similarly provides general protection through Articles 4, 7, 19, and 23, which recognise the consumer's rights to security, compensation, reimbursement, and access to dispute resolution, while Article 18 paragraph (1)(a) prohibits standard-form clauses that transfer business responsibility to consumers. Nevertheless, these provisions do not specifically regulate reporting periods, reimbursement deadlines, evidentiary standards, or the allocation of losses among issuers, acquirers, merchants, switching institutions, and consumers (Saraswati et al., 2026). Bank Indonesia Regulation Number 3 of 2023 further establishes fair treatment, responsible business conduct, protection of consumer assets, and effective complaint resolution, while Bank Indonesia Regulation Number 10 of 2025 and Board of Governors Regulation Number 32 of 2025 strengthen payment-system governance, technological infrastructure,

market conduct, and fraud management. However, these general statutory and regulatory obligations have not yet developed into a complete and operational liability regime, particularly with respect to the timing of notification, complaint resolution, and reimbursement for unauthorized QRIS transactions (Satriatama & Dikrurahman, 2026).

The consumer-protection framework has subsequently been updated through Bank Indonesia Regulation Number 6 of 2026 on Bank Indonesia Consumer Protection, which repealed and replaced Bank Indonesia Regulation Number 3 of 2023 (Marianingsih et al., 2026). The current regulation reinforces fair treatment, responsible business conduct, protection of consumer assets, and effective complaint handling. Importantly, Article 47 places responsibility for proving the relevant elements of fault or negligence upon the provider and expressly recognises shared responsibility where both the provider and the consumer are at fault. These developments provide a substantive foundation for assessing liability for unauthorized QRIS transactions.

Complaint handling is now regulated by Bank Indonesia Board of Governors Member Regulation Number 32 of 2026 concerning Procedures for the Implementation of Bank Indonesia Consumer Protection. Article 42(b) requires written complaints concerning suspected regulatory violations or operational failures causing actual or potential financial loss to be resolved within ten business days after all submission requirements have been fulfilled. For operational-failure complaints, Article 42(c)–(e) permits extensions under specified conditions, subject to prior written notification. Fraud-related complaints are governed separately by Article 43, which requires an immediate initial response once the submission requirements are fulfilled and an in-depth investigation within twenty business days. Under Article 43(4)–(5), an extension is permitted where necessary follow-up by another party beyond the

provider's control affects resolution, provided that written notice is given before the investigation period expires. Consumers dissatisfied with the provider's resolution may submit a complaint to Bank Indonesia, subject to the documentary requirements under Article 101. For complaints involving actual or potential financial loss, Article 103 requires submission within sixty business days from the date on which the provider communicates its written resolution to the consumer.

Although the foregoing provisions prescribe time limits for handling and resolving consumer complaints, they essentially establish only procedural periods within which service providers must examine, verify, and respond to such complaints. The prevailing regulatory framework does not prescribe a substantive deadline within which a service provider must reimburse funds lost as a result of an unauthorized QRIS transaction. Nor does it correlate the promptness of the consumer's report with the extent of liability borne by each party. In other words, the existing framework does not determine how a delay in reporting affects the allocation of losses incurred before and after notification is given to the service provider.

Establishing a legal relationship between the timing of notification and the allocation of liability is essential to achieving a balanced system of legal protection. On the one hand, consumers should not be permitted to report an unauthorized transaction after an unlimited period, particularly where such delay has resulted in additional losses that could otherwise have been prevented. In such circumstances, an unjustified delay in reporting may reasonably be regarded as the consumer's contributory conduct in the aggravation of the loss. On the other hand, the service provider must remain obligated to reimburse the consumer where the consumer has acted in good faith, exercised reasonable care in safeguarding payment credentials, and reported the unauthorized transaction within a reasonable period. Accordingly, a regulatory framework is required to allocate liability on a graduated basis by

reference to the promptness of notification, the degree of fault attributable to each party, the causal relationship between the relevant conduct and the resulting loss, and the respective capacity of each party to prevent or mitigate such loss.

As a comparative reference, the United States expressly regulates the relationship between the timing of consumer notification and the extent of consumer liability for unauthorized electronic fund transfers under the Electronic Fund Transfer Act, as implemented through Regulation E, particularly 12 C.F.R. §§ 1005.6 and 1005.11 (Callaway, 2022). Although Regulation E is not specifically designed for QR-code payments, it provides a relevant functional comparison because it establishes an operational liability framework for unauthorized electronic transfers. Under § 1005.6(b), consumer liability is determined through graduated tiers based principally on the promptness of notification. Where a consumer notifies the financial institution within two business days after learning of the loss or theft of an access device, the consumer's liability is generally limited to the lesser of USD 50 or the amount of unauthorized transfers occurring before notification (Kierner et al., 2026). Where notification is made after the two-business-day period, liability may increase to a maximum of USD 500, consisting of the initial limited amount and additional losses that the financial institution proves would not have occurred had timely notification been given. If an unauthorized transfer appears on a periodic statement and the consumer fails to report it within sixty days after the statement is transmitted, the consumer may also bear subsequent losses that the institution proves could have been prevented through timely notification. Regulation E further provides that ordinary consumer negligence cannot be used, whether contractually or otherwise, to impose liability exceeding the prescribed regulatory limits (Selznick & LaMacchia, 2015).

These comparative frameworks demonstrate that time may operate not merely as a procedural deadline for complaint handling, but as a substantive criterion for

allocating loss, determining the consumer's maximum exposure, triggering provisional or immediate reimbursement, and defining the financial institution's evidentiary burden. Unlike the United States and the European Union, Indonesia has not yet expressly incorporated such a time-sensitive and graduated allocation of liability into its QRIS regulatory framework. Indonesian regulations prescribe periods for processing and resolving consumer complaints, but do not specifically determine how prompt or delayed notification affects consumer liability, which losses occurring after notification must be borne by the provider, or when disputed funds must be provisionally or finally restored.

Against this regulatory backdrop, the principal deficiency in Indonesia's treatment of unauthorized QRIS transactions does not lie in the complete absence of legal protection, but in the absence of a liability regime that expressly connects the timing of notification, the obligation to reimburse disputed funds, the degree of fault, causal contribution, and the respective capacity of each party to prevent or mitigate loss. This condition creates legal uncertainty for both consumers and service providers. Consumers who have exercised due care and promptly reported an unauthorized transaction are not yet guaranteed restoration of their funds within a specified period, while service providers likewise lack a clear normative basis for limiting their liability where a consumer's delayed notification can be shown to have caused or aggravated subsequent losses.

Accordingly, Indonesia requires a legal-policy formulation that integrates the *time-bound tiered liability doctrine* into the QRIS regulatory framework by allocating liability on a graduated basis according to the promptness of notification, the degree of fault, causal contribution, and control over the relevant risk. Such a formulation is expected to realise proportional justice by affording full protection to consumers who act in good faith and comply with their duty of care, while simultaneously providing

reasonable protection to service providers against additional losses attributable to unjustified delay or consumer negligence. On that basis, this study is necessary to examine the characteristics and deficiencies of Indonesia's existing liability framework governing unauthorized QRIS transactions and to formulate a regulatory model that is more certain, balanced, and operational.

Based on the foregoing, the legal issues addressed in this article are formulated as follows:

1. How does the current regulatory framework govern legal liability and consumer compensation concerning unauthorized electronic transactions within the Indonesian QRIS ecosystem?
2. How should a legal policy be formulated to optimally integrate the time-bound tiered liability doctrine into Indonesia's QRIS regulatory framework?

Although previous studies have examined consumer protection, fraud prevention, and comparative payment regulation within the QRIS ecosystem, further analysis is needed to determine how notification timing, consumer fault, and preventable loss should be integrated into a coherent framework of liability and reimbursement. First, the article by Tara and Sudiro (2023), entitled "Perindungan Hukum Konsumen Terhadap Pengguna Qris dan Penanganan Penipuan dalam Bertransaksi," examines the legal protection available to QRIS users and responses to fraudulent transactions (Tara & Sudiro, 2023b). Through normative legal research, the authors recommend preventive protection through consumer education, repressive protection through stronger law enforcement, and issuer responsibility for losses arising from internal system problems. Their analysis establishes that consumer protection requires both fraud prevention and mechanisms for holding providers accountable. However, it does not formulate reporting periods linked to consumer

liability limits, distinguish initial losses from preventable additional losses, or specify provisional reimbursement deadlines. These limitations identify an operational question that the present study addresses: how responsibility should be allocated when a consumer's delayed notification contributes to further unauthorized transactions. Accordingly, this study extends their general protective framework by connecting notification time, fault, causation, and preventable loss within the proposed Time-Bound Tiered Liability Doctrine.

Second, the article by Sitanggang and Haryanto (2025), entitled "QRIS as a Single Payment Gateway as a Solution for Payment Efficiency and Legal Protection for e-commerce Consumers Through a Comparison With China," investigates weaknesses in payment integration and consumer protection through statutory analysis and comparison with China (Sitanggang & Haryanto, 2025). The authors identify technological and regulatory shortcomings and recommend improved interoperability, stronger transaction security, and dedicated e-commerce legislation. Their comparative contribution concerns the infrastructure and regulatory conditions supporting integrated payments, rather than the allocation of losses following unauthorized transactions. They do not develop notification-based liability tiers or rules governing reimbursement while an investigation remains pending. The present study therefore addresses a more specific gap in Indonesia's framework: the absence of an explicit connection between reporting delay, quantified consumer liability, and reimbursement obligations for unauthorized QRIS transactions. Building on existing recognition of shared responsibility, its novelty lies in functionally adapting principles from United States Regulation E and European Union payment-services rules into an operational model that distinguishes initial loss from preventable additional loss, limits delay-related consumer liability through proof of causation, and requires provisional reimbursement.

2. Research Method

This study employs normative legal research to examine the rules governing liability and compensation for unauthorized transactions within Indonesia's Quick Response Code Indonesian Standard (QRIS) ecosystem and to formulate the proposed Time-Bound Tiered Liability Doctrine. It applies statutory, conceptual, and comparative approaches (Khadapi et al., 2023). These approaches are used to establish the applicable legal position, clarify the concepts underlying loss allocation, and assess alternative regulatory mechanisms for protecting consumers while maintaining proportionate provider responsibility.

The primary legal materials comprise Indonesian legislation and regulations governing electronic transactions, consumer protection, payment services, and QRIS implementation. They include Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 1 of 2024; Law Number 8 of 1999 on Consumer Protection; Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions; Bank Indonesia Regulation Number 10 of 2025 on Payment System Industry Regulation and its implementing Board of Governors Member Regulation Number 32 of 2025; Bank Indonesia Regulation Number 6 of 2026 on Bank Indonesia Consumer Protection; and Board of Governors Member Regulation Number 32 of 2026 on Procedures for Implementing Bank Indonesia Consumer Protection. The QRIS-specific materials include Board of Governors Member Regulation Number 21/18/PADG/2019 on the Implementation of the National Quick Response Code Standard for Payments and its amendments, including Regulation Number 3 of 2025. Superseded provisions are considered where necessary to explain regulatory developments, while the assessment of current obligations relies on the applicable rules.

The comparative primary materials comprise United States Regulation E,

particularly 12 C.F.R. §§ 1005.2(m), 1005.6, and 1005.11, and Directive (EU) 2015/2366, particularly Articles 69–74. These instruments are selected for their functional relevance to unauthorized electronic payments, notification duties, liability limits, evidentiary requirements, and reimbursement. Official explanatory notes and regulatory interpretations support the interpretation of these instruments, with attention to their respective legal status.

Secondary legal materials consist of books, peer-reviewed journal articles, legal commentaries, and research reports concerning QRIS, unauthorized electronic transactions, consumer protection, payment-system liability, and comparative financial regulation. Materials are collected through documentary and literature studies and selected purposively according to their relevance to the research questions, legal authority or scholarly credibility, temporal applicability, and contribution to explaining the concepts or regulatory mechanisms examined. Recent scholarship is prioritised while retaining foundational works. Legislative texts and regulatory interpretations are checked against official publications to establish their authenticity, amendment history, and applicability.

The analysis proceeds through three connected procedures. Under the statutory approach, relevant provisions are identified and classified according to provider obligations, consumer duties, notification requirements, fault, burdens of proof, complaint handling, and compensation. Their scope and consistency are examined through textual and systematic interpretation, taking account of the hierarchy and relationship between general and sector-specific rules. Under the conceptual approach, the study distinguishes consent from technical authentication, ordinary negligence from gross negligence and intentional misconduct, and initial loss from additional loss preventable through timely notification. Under the comparative approach, Indonesian, United States, and European Union rules are examined against

common functional questions: when notification duties arise, how delay affects liability, which party must establish fault and causation, and when disputed funds must be restored. Differences in institutional arrangements and regulatory scope are considered when assessing the suitability of foreign mechanisms for QRIS.

The findings are synthesised qualitatively and prescriptively through legal interpretation and legal construction. The proposed doctrine builds on existing rules concerning provider liability, shared responsibility, and evidentiary burdens by specifying their relationship with notification timing and preventable additional loss. The proposed rules are assessed against legal certainty, proportional justice, consumer protection, causal fairness, and compatibility with the legal duties and institutional functions of payment service providers. The reporting thresholds and liability percentages constitute normative policy recommendations informed by this analysis, rather than empirically validated estimates.

3. Results and Discussion

A. Characteristics and Regulatory Gaps in Legal Liability and Consumer Compensation for Unauthorized Transactions in Indonesia's QRIS Ecosystem

1. The Characteristics of Legal Liability and Consumer Compensation for Unauthorized QRIS Transactions

The legal framework governing liability and compensation for unauthorized QRIS transactions in Indonesia does not amount to an absolute regulatory vacuum. Indonesian law already provides several legal bases for assessing the responsibility of consumers, Payment Service Providers (*Penyedia Jasa Pembayaran* or PJP), Electronic System Providers (*Penyelenggara Sistem Elektronik* or PSE), and business actors (*pelaku usaha*) (Pattynama et al., 2024). Nevertheless, these rules are dispersed across several bodies of law and were not specifically designed as a dedicated liability regime for unauthorized QRIS

transactions. The central problem, therefore, is not the absence of legal rules, but their dispersed and incomplete character in governing risk allocation, evidentiary matters, and consumer redress.

At the level of electronic-system governance, Article 15 paragraphs (1) and (2) of Law Number 11 of 2008 on Electronic Information and Transactions, as last amended by Law Number 1 of 2024 (*Undang-Undang Informasi dan Transaksi Elektronik* or the EIT Law), requires every PSE to operate its electronic system reliably and securely and to assume responsibility for its proper operation (Hamzah Muchtar et al., 2024a). These provisions may serve as a basis for holding a PJP liable where an unauthorized QRIS transaction results from defective authentication, inadequate access controls, an application vulnerability, an undetected account takeover, or another failure within the provider's system. Article 15 paragraph (3) permits an exception where the provider proves force majeure or fault and/or negligence on the part of the user. Accordingly, a provider should not be released from liability merely because the transaction record indicates the use of a PIN, biometric verification, a one-time password, or a registered device. The provider must still demonstrate that its system operated reliably and securely and that the loss was in fact caused by the user's fault (Aurora et al., 2026).

Article 21 of the EIT Law further allocates legal consequences according to the mechanism through which an electronic transaction is performed. Where a transaction is conducted through an Electronic Agent (*Agen Elektronik*), its legal consequences are borne by the operator of that Electronic Agent. Losses arising from the failure of an Electronic Agent caused by a direct third-party action against the electronic system are likewise attributed to the Electronic Agent operator. Conversely, where the failure is caused by the user's negligence,

responsibility rests with the user. Within the QRIS ecosystem, *mobile-banking* applications, electronic wallets, and other automated payment facilities may be analysed as part of the operation of an Electronic Agent. Article 21, however, does not specify the applicable standard of user negligence, distinguish ordinary negligence from gross negligence, define the causal relationship between negligence and loss, or prescribe the maximum loss that may be allocated to the consumer.

The provider's obligations are reinforced by Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions (*Penyelenggaraan Sistem dan Transaksi Elektronik*). Article 36 provides that an Electronic Agent forms part of an electronic system and that the obligations governing electronic-system operation therefore apply *mutatis mutandis* to an Electronic Agent operator. Article 39 requires the application of the principles of prudence, system security and integrity, security controls, efficiency, and consumer protection. Article 40 paragraph (1) further requires an Electronic Agent operator to authenticate the user's identity and verify authorisation, adopt policies for indications of data theft, control authorisation and access rights, protect the integrity of transaction data, and maintain procedures for the prompt and appropriate handling of incidents, fraud, and system failures. These provisions provide a basis for assessing whether a PJP has exercised due care in preventing unauthorized transactions, but they do not operationally regulate the financial consequences that must follow once an unauthorized transaction has been reported.

The consumer-protection regime also provides a basis for balancing rights and obligations. Article 2 of Law Number 8 of 1999 on Consumer Protection (*Undang-Undang Perlindungan Konsumen* or the Consumer Protection Law)

identifies fairness, balance, security, safety, and legal certainty as the governing principles of consumer protection. Article 4(a) grants consumers the right to comfort, security, and safety in the use of goods or services, while Article 4(h) recognises the right to compensation, indemnification, and/or replacement where the services received are inconsistent with the agreement or are not provided as they should be (Yana et al., 2026). These rights are balanced by the consumer obligations under Article 5, including the duties to read and comply with instructions for use, act in good faith, and participate in the proper resolution of consumer disputes.

This balance is also reflected in the rights of business actors under Article 6 of the Consumer Protection Law, including the right to legal protection against consumers acting in bad faith, the right to defend themselves, and the right to restoration of reputation where it is established that the consumer's loss was not caused by the goods or services supplied. Conversely, Article 7(f) and (g) requires business actors to provide compensation or indemnification for losses arising from the use of their services and where the services received do not conform to the agreement. Article 18 paragraph (1)(a) prohibits standard-form clauses that transfer the responsibility of a business actor to the consumer. A PJP may therefore not unilaterally rely on its terms and conditions to shift the entire risk of unauthorized QRIS transactions to consumers (Agustin et al., 2025).

Article 19 paragraphs (1) and (2) of the Consumer Protection Law provide that business actors are responsible for compensating consumer losses and that compensation may take the form of a refund or the replacement of goods or services with an equivalent kind or value. Article 19 paragraph (3) further states that compensation must be provided within seven days of the transaction date. Article 19 paragraph (5), however, allows a business actor to avoid liability

where it proves that the loss was caused by the consumer's fault. Where the business actor refuses, fails to respond to, or fails to satisfy a claim for compensation, Article 23 permits the consumer to bring a claim before the Consumer Dispute Settlement Agency (*Badan Penyelesaian Sengketa Konsumen* or *BPSK*) or a competent court. In compensation proceedings, Article 28 places the burden of proving the presence or absence of fault upon the business actor (Matthew Jakaria Sitanggang & Imam Haryanto, 2025).

Although Article 19 paragraph (3) of the Consumer Protection Law prescribes a seven-day period, that provision cannot be equated with a reimbursement mechanism for unauthorized QRIS transactions (Sasra & Baidhowi, 2025). First, the period runs from the date of the transaction rather than from the date on which the consumer discovers and reports the unauthorized transaction. A consumer may only become aware of the misuse after receiving a notification, reviewing the transaction history, or obtaining an account statement. Second, Article 19 does not regulate the technical investigation process, provisional credit, the status of the disputed funds during the investigation, or the allocation of responsibility among the issuer, acquirer, merchant, and switching institution. Third, the provision assumes that the responsible business actor can already be identified, whereas the source of failure within the QRIS ecosystem may lie at several stages of transaction processing. Article 19 therefore supplies a general basis for compensation, but it does not establish an operational procedure for restoring funds lost through unauthorized QRIS transactions (Zulia Ramdhani et al., 2025).

Within the payment-system framework, Bank Indonesia Regulation Number 6 of 2026 on Bank Indonesia Consumer Protection (*Peraturan Bank Indonesia tentang Pelindungan Konsumen Bank Indonesia*), which repealed and

replaced Bank Indonesia Regulation Number 3 of 2023, reinforces these protections. Article 5 paragraph (1) establishes the principles of transparency, fair treatment and responsible business conduct, protection of consumer assets, privacy and data, and effective and efficient complaint handling and dispute resolution. Article 4 letter (a) identifies legal certainty and effective and efficient complaint handling and dispute resolution as regulatory objectives. Article 39 paragraphs (1) and (2) further require providers to safeguard consumer assets, privacy, and data within their responsibility and to establish and implement appropriate protection mechanisms.

Article 46 paragraph (4) requires providers to assume responsibility for consumer losses arising from fault, negligence, or unlawful conduct committed by their management, employees, or relevant third parties supporting the provision of their products or services. In compensation claims, Article 47 paragraph (1) places responsibility for proving the presence or absence of such conduct upon the provider. Article 47 paragraph (2) permits release from liability where consumer fault, negligence, or unlawful conduct is proven, while paragraph (3) expressly recognises shared responsibility where both the provider and the consumer are at fault. Article 13 recognises consumers' rights to submit complaints, obtain protection and dispute resolution, and receive compensation under the applicable conditions. Article 14 sets out corresponding duties, including good faith, accurate disclosure, compliance with agreements, and protection of security credentials and authentication information. The framework therefore recognises both individual and shared responsibility. The remaining issue examined in this article concerns how shared responsibility should be translated into predictable loss allocation according to notification timing, causal contribution, and the extent to which

additional losses could have been prevented.

The normative foundation for the proposed doctrine lies in connecting existing provider obligations with a more specific allocation of causally attributable losses. Articles 15 and 21 of the EIT Law establish responsibility concerning electronic-system operation and user negligence, while Article 19 of the Consumer Protection Law provides a general basis for compensation and an exception where consumer fault is established. Article 47 of Bank Indonesia Regulation Number 6 of 2026 further places the evidentiary burden on the provider and recognises shared responsibility where both parties are at fault. These provisions support an inquiry into each party's contribution to the loss, but do not themselves prescribe notification-based liability ceilings. The proposed doctrine would supply those operational parameters while requiring their harmonisation with existing statutory rules on fault and compensation.

Notification time should therefore operate as an indicator requiring further examination, rather than as conclusive proof of consumer negligence. Before allocating additional loss to the consumer, the PJP should establish when the consumer knew or reasonably ought to have known of the unauthorized transaction, whether reporting was reasonably possible, which subsequent losses occurred, and what effective preventive action timely notification would have enabled. The relevant causal question is whether an identifiable additional loss would have occurred if the consumer had reported within the applicable period. A completed initial transaction cannot retrospectively become a consequence of later reporting delay. Any responsibility for that initial loss must be assessed separately by reference to the conduct that caused it. This approach draws on Regulation E's requirement that institutions establish the preventability of specified subsequent transfers. Under the proposed model,

responsibility for losses caused by the PJP's failure to act after effective notification should remain with the PJP.

Bank Indonesia Regulation Number 10 of 2025 on Payment System Industry Regulation (Pengaturan Industri Sistem Pembayaran) also requires payment systems to be operated in a fast, accessible, affordable, secure, and reliable manner while maintaining consumer protection. Its scope encompasses governance, risk management, information-technology infrastructure, market conduct, and consumer protection. Meanwhile, Board of Governors Regulation Number 3 of 2025, which constitutes the third amendment to the national QRIS implementation rules, expands the technical and operational framework for QRIS, including its use models, data-communication technology, funding sources, and cross-border transactions. The prevailing QRIS rules, however, remain directed primarily at technical standardisation, interoperability, and transaction processing rather than at establishing a dedicated regime for unauthorized transactions and reimbursement.

The characteristics of the prevailing framework may therefore be summarised as follows. First, the legal bases for liability are drawn from several bodies of law, including electronic-systems law, consumer-protection law, and payment-system regulation (Ayuningtyas et al., 2024). Second, liability is assessed by reference to system reliability, fault, negligence, and causation. Third, the liability structure involves several participants, including issuers, acquirers, merchants, switching institutions, and supporting providers. Fourth, the law recognises both the consumer's right to compensation and the provider's right to be released from liability where the consumer is proven to have caused the loss. Fifth, the rules remain focused on prevention, system security, and complaint handling rather than on a time-sensitive allocation of losses. Research

on digital consumer protection in Indonesia likewise indicates that the existence of several legal bases has not eliminated uncertainty and regulatory gaps in increasingly complex digital consumer relationships.

2. *The Normative Gap Concerning Notification Periods and Reimbursement, and Its Legal Consequences*

The clearest regulatory gap in Indonesia concerns the relationship between the time of notification and the legal consequences of the resulting loss. Article 30(b) of Bank Indonesia Board of Governors Regulation Number 20 of 2023 on Procedures for the Implementation of Bank Indonesia Consumer Protection (*Peraturan Anggota Dewan Gubernur tentang Tata Cara Pelaksanaan Pelindungan Konsumen Bank Indonesia*) requires a provider to resolve a written complaint within twenty business days after the complaint and all supporting documents have been received in complete form. Article 30(c) permits an extension of up to a further twenty business days. Under Article 30(d), the extension may exceed that period where resolution requires follow-up action by another party beyond the provider's control, subject to the written-notification requirement in Article 30(e).

These periods are merely procedural deadlines within which a provider must examine, verify, and respond to a complaint. They do not establish a specific period within which a consumer must report an unauthorized QRIS transaction after the consumer knew or reasonably ought to have known of it. Nor do they determine when a PJP must provide provisional reimbursement, when reimbursement must become final, or how delayed notification affects the allocation of losses incurred before and after notice is given (Hamzah Muchtar et al., 2024b).

Accordingly, the proposition that Indonesia has 'no time limit' must be understood in a limited and precise sense. Indonesia already prescribes a period

for providers to resolve complaints and a general time limit for compensation under the Consumer Protection Law. It does not, however, establish a specific prompt-notification period governing when a consumer must report an unauthorized QRIS transaction and connecting the promptness of that report to graduated liability. Nor does Indonesia prescribe a substantive deadline specifically requiring restoration of funds lost through an unauthorized transaction, whether by provisional credit or final reimbursement (Hamka et al., 2026).

A further weakness lies in the absence of a distinction between losses incurred before notification and additional losses incurred after the consumer should have given notice. The prevailing rules do not determine whether a consumer who reports within a few hours should be treated in the same manner as a consumer who waits several days or months. They also fail to specify whether delayed notification extinguishes the entire right to reimbursement, reduces reimbursement in part, or renders the consumer liable only for additional losses that are proven to have been preventable through timely notification (Mulia & Bangsawan, 2025).

There is likewise no maximum limit on consumer liability according to the degree of negligence. The provisions examined do not themselves prescribe quantified caps on consumer liability differentiated by degree of fault. Articles 15 and 21 of the EIT Law and Article 19 paragraph (5) of the Consumer Protection Law recognise fault or negligence as relevant to the allocation of responsibility, but do not establish distinct financial consequences for ordinary negligence, gross negligence, and intentional misconduct. Under Bank Indonesia Regulation Number 6 of 2026, Article 46 paragraph (4) establishes provider responsibility for losses attributable to specified persons acting within

or in support of its operations, while Article 47 places the evidentiary burden on the provider, permits exemption where consumer fault is proven, and recognises shared responsibility where both parties are at fault. Nevertheless, these provisions do not specify liability caps corresponding to different degrees of consumer fault or a formula for apportioning losses. This distinction matters because an inadvertent mistake in using payment technology should not automatically attract the same consequences as fraudulent collusion or deliberate misuse of a payment instrument. Disclosure of a PIN or other security credential should therefore be assessed in context, including any deception, the consumer's conduct, its causal contribution to the loss, and failures attributable to the provider. Comparative approaches offer different safeguards: Article 74 of Directive (EU) 2015/2366 links liability beyond the ordinary cap to fraud or intentional or grossly negligent breaches of specified obligations, whereas United States Regulation prevents consumer negligence from increasing liability beyond its prescribed limits. These approaches support clearer differentiation of fault and liability limits in the proposed Indonesian model.

This distinction is material because a minor error in the use of payment technology should not necessarily produce the same legal consequences as deliberately disclosing a PIN, colluding with a fraudster, or repeatedly disregarding security warnings. International literature on unauthorized payment transactions similarly treats proof of fraud or gross negligence as an important threshold before losses may be shifted from the payment service provider to the consumer.

Against this background, at least three legal problems arise from the absence of a notification period for unauthorized QRIS transactions that is integrated with the allocation of liability, the amount of compensation, and the

duty to reimburse funds.

First, there is no legal certainty regarding the period within which a consumer must submit a report. The absence of a specific period for reporting an unauthorized QRIS transaction allows a consumer to submit a report at an indeterminate time after the transaction occurred or became known. In practical terms, the consumer appears to have an unlimited period within which to report the transaction.

This creates uncertainty for PJPs because the longer notification is delayed, the more limited the provider's ability becomes to trace the transaction, secure the account, block the payment instrument, contact the merchant, and prevent further loss. In certain circumstances, delayed notification may also result in the loss or deterioration of electronic evidence required to identify the source of the failure and the responsible party.

A notification period is also necessary to give operational meaning to the consumer's duty to prevent and limit loss. Consumer protection creates not only a right to reimbursement, but also a duty to act in good faith and promptly notify the provider of an unrecognised transaction. Delayed notification should not, however, automatically extinguish the consumer's entire right to compensation. Legal consequences should arise only where the PJP proves that the consumer knew or reasonably ought to have known of the unauthorized transaction, delayed notification without a justifiable reason, and thereby directly caused additional losses that could otherwise have been prevented (Mumtakhinah et al., 2026).

Second, there is no certainty regarding the amount of compensation or the financial liability borne by each party. A PJP cannot determine at the outset whether the entire loss must be reimbursed, whether part of the loss may be

allocated to the consumer, or whether the consumer's responsibility is confined to subsequent transactions that could have been prevented. The consumer likewise lacks certainty as to the amount of funds that will be restored. Consequently, cases with comparable characteristics may result in different amounts of reimbursement depending on the internal policy of the relevant PJP.

Uncertainty regarding the amount of compensation also impairs the provider's ability to plan for and manage losses. PJPs lack uniform legal parameters for estimating loss reserves, allocating responsibility among participants in the QRIS transaction chain, or seeking recourse against an acquirer, merchant, switching institution, or technology provider. At the same time, a consumer may be required to bear the entire loss merely because the transaction record shows the use of valid credentials, without an adequate assessment of whether those credentials were lawfully used or whether the provider's system was capable of detecting anomalous activity. The absence of a clear liability limit therefore creates uncertainty not only for consumers, but also for providers acting in good faith.

Third, uncertainty concerning proof and causation may produce inconsistent outcomes. The longer an unauthorized transaction remains unreported, the more difficult it becomes for the parties to reconstruct the relevant events accurately. Device data may change, electronic communications may be deleted, credentials may be used repeatedly, funds may be transferred through several accounts, and subsequent unauthorized transactions may become intermingled with authorised transactions. In those circumstances, it becomes difficult to distinguish the initial loss falling within the provider's sphere of control from additional loss arising from the consumer's delayed notification.

The absence of specific rules may also lead technical authentication to be treated improperly as conclusive proof of consent. The recorded use of a PIN or biometric verification should constitute only one item of evidence; it should not automatically establish that the consumer knowingly authorised the transaction. Conversely, a consumer should not be released from every consequence where the provider proves that unjustified delay caused preventable subsequent transactions. Without standards governing time, the burden of proof, gross negligence, and causation, the outcome of a complaint will depend heavily on the interpretation and internal policies of the PJP concerned. International literature indicates that uncertainty and inconsistency as to when consumers bear liability may increase perceived risk, reduce confidence in payment services, and intensify demands for greater security.

These three consequences demonstrate a failure to secure legal certainty in two respects. At the normative level, there are no clear, specific, and predictable rules governing when a report must be submitted, when funds must be restored, and what proportion of the loss must be borne by each party (Purwanto et al., 2025). At the level of implementation, comparable cases may produce different outcomes because their resolution depends on the terms and conditions and investigative policies adopted by each PJP. This position is inconsistent with the principles of legal certainty and balance under Article 2 of the Consumer Protection Law and with the objective of Bank Indonesia Regulation Number 6 of 2026 to secure legal certainty and effective complaint resolution (Syahrin et al., 2025).

The legal gap within the QRIS ecosystem therefore concerns more than the absence of a reporting deadline. It lies in the absence of a normative relationship among the timing of notification, the consumer's duty to mitigate loss, the PJP's

duty to reimburse funds, the applicable limits of liability, and proof of causation. An appropriate regulatory model should provide full protection to consumers who report promptly and exercise due care, while protecting PJPs against additional losses proven to have arisen from unjustified consumer delay. This need provides the basis for the *Time-Bound Tiered Liability Doctrine* as a model of loss allocation that is more certain, proportionate, and operational.

B. The Ideal Formulation of the Time-Bound Tiered Liability Doctrine within Indonesia's QRIS Regulatory Framework

1. The United States Framework for Liability for Unauthorized Electronic Transactions

The United States provides a relevant point of comparison for allocating liability for unauthorized QRIS transactions because it regulates in detail the relationship between the timing of notification and the extent of consumer liability. The relevant rules are contained in the *Electronic Fund Transfer Act* and its implementing regulation, *Regulation E*, codified in 12 C.F.R. Part 1005. Although *Regulation E* was not specifically designed for QR-code payments, it performs a comparable legal function by protecting consumers against electronic fund transfers undertaken without their authorisation. It therefore offers a useful functional comparison for developing a liability framework for unauthorized QRIS transactions in Indonesia.

Section 1005.2(m) of *Regulation E* defines an *unauthorized electronic fund transfer* as an electronic fund transfer from a consumer's account initiated by a person other than the consumer, without actual authority, and from which the consumer receives no benefit (Patterson, 2022). The definition is important because it confines the protective regime to transactions that were genuinely not

authorised. A transaction undertaken by the consumer, even where the consumer acted because of deception or false information, raises a legally distinct issue. This distinction prevents the reimbursement mechanism from being applied to every payment dispute without determining whether the consumer actually authorised the transaction.

The allocation of consumer liability is governed by 12 C.F.R. § 1005.6. The provision essentially establishes three tiers of liability based on the timing of notification (Sanchez-Adams, 2024). The first tier applies where the consumer notifies the financial institution of the loss or theft of an access device within two business days after learning of it. In that circumstance, the consumer's liability is limited to the lesser of USD 50 or the amount of unauthorized transfers occurring before notice was given.

The second tier applies where the consumer gives notice after the two-business-day period but within 60 calendar days after the first periodic statement showing the unauthorized transfer was transmitted. Consumer liability may then increase to a maximum of USD 500. The financial institution may not, however, automatically allocate the entire loss to the consumer. It must prove that the additional transfers occurring after the two-business-day period would not have occurred had the consumer given timely notice (Budnitz, 2025).

The third tier applies where the consumer fails to notify the financial institution within 60 days after the periodic statement was transmitted. The consumer may be held liable for subsequent transfers occurring after the expiry of the 60-day period and before notice is ultimately given. Such liability remains conditional upon proof by the financial institution that the subsequent transfers could have been prevented had notice been provided within the prescribed period. Delay therefore does not automatically require the consumer to bear

every transaction from the outset. Liability is directed principally towards additional losses that are causally connected to delayed notification.

This framework assigns two functions to the timing of notification. First, it encourages consumers to notify the financial institution promptly of a lost access device or an unrecognised transaction. Second, it determines the maximum loss that may be allocated to the consumer. The more promptly notice is given, the lower the consumer's liability. Conversely, delayed notice may increase liability only where the financial institution proves that the delay caused additional loss.

Another significant feature is that ordinary consumer negligence cannot be used to impose liability beyond the limits prescribed by *Regulation E*. The Official Interpretations to § 1005.6 explain that writing a PIN on a card, or on a document kept with the card, does not by itself increase consumer liability beyond the regulatory limit. Nor may an agreement between the financial institution and the consumer impose liability more onerous than that permitted under *Regulation E*. These restrictions prevent financial institutions from using standard-form terms to transfer the entire risk of unauthorized transactions to consumers.

Consumers nevertheless remain subject to a duty to provide proper notice. Notice is treated as given when the consumer takes steps reasonably necessary to provide the financial institution with the relevant information. It may be provided in person, by telephone, or in writing. *Regulation E* also recognises extenuating circumstances that prevent timely notice, including hospitalisation or extended travel. In such circumstances, the notification period must be extended for a reasonable period. This qualification demonstrates that time limits should not be applied rigidly without regard to the consumer's actual

circumstances.

In addition to allocating liability, *Regulation E* distinguishes the period for investigating an error from the restoration of the consumer's funds. Under 12 C.F.R. § 1005.11, an unauthorized electronic fund transfer constitutes an error that must be investigated by the financial institution. As a general rule, the institution must complete its investigation within ten business days. Where the investigation cannot be completed within that period, it may be extended, generally for up to 45 days, provided that the institution provisionally credits the consumer's account within ten business days. The consumer must be permitted to use the provisionally credited funds while the investigation remains pending.

Where the financial institution subsequently determines that an error occurred, it must correct the error within one business day. If no error is found, the institution must provide a written explanation and notify the consumer of the right to request the documents relied upon in the investigation. This mechanism prevents consumers from being deprived of access to their funds throughout a lengthy investigation, while preserving the institution's ability to reverse the provisional credit where the evidence establishes that the transaction was authorised.

2. *A Proposed Model for the Time-Bound Tiered Liability Doctrine in Indonesia*

On the basis of this comparison, Indonesian regulation should connect the timing of notification with a graduated allocation of liability. This article refers to the proposed model as the Time-Bound Tiered Liability Doctrine. The doctrine is a legal-policy proposal rather than a doctrine currently recognised in Indonesian positive law. The time-bound element means that legal consequences are determined by the period running from the time at which the

consumer knew or reasonably ought to have known of the unauthorized transaction. The tiered-liability element means that liability is not invariably imposed in full upon one party, but is allocated in graduated proportions according to the timing of notification, the degree of fault, causation, and each party's capacity to prevent the loss.

Before establishing the tiers of liability, the regulation must provide a clear definition of an unauthorized payment transaction. An unauthorized QRIS transaction should be defined as a transaction that debits the consumer's funding source, is undertaken without valid consent by a person lacking authority, and confers no benefit upon the consumer. This category should be distinguished from an erroneous transfer, a processing failure, a dispute concerning goods or services, and a transaction performed by the consumer as a result of deception. The distinction is necessary because each event gives rise to a different basis of liability and a different form of redress.

The doctrine must also determine when the notification period begins to run. Time should not be calculated solely from the transaction date because the consumer may not immediately become aware of the misuse. The period should begin when the consumer actually knew or reasonably ought to have known of the unauthorized transaction, as evidenced by a notification, account statement, transaction history, or communication from the PJP. Where the PJP fails to issue a notification, or the notification is received late, the resulting delay should not be attributed to the consumer.

As an initial formulation, liability may be allocated across four tiers. The percentages proposed for each tier are normative recommendations that Bank Indonesia may adjust by reference to transaction data, fraud rates, and the capacity of the payment-system industry.

The proposed reporting periods constitute normative policy choices intended to balance prompt intervention, reasonable opportunities to report, and proportionate allocation of preventable loss. To maintain sequential and non-overlapping intervals, the model uses calendar time: within 24 hours; after 24 hours up to three calendar days; after three up to seven calendar days; and after seven up to 60 calendar days. These periods run from the consumer's actual or reasonably attributable awareness of the unauthorized transaction, subject to proof by the PJP and reasonable extensions where reporting was genuinely prevented. Crossing a threshold changes the applicable liability ceiling; it does not independently establish negligence or causation.

The first tier provides full reimbursement for notification within 24 hours, subject to consistently defined exceptions for proven fraud or intentional misconduct. Its justification rests on encouraging rapid notification while recognising that consumers require a practical opportunity to identify and report an unfamiliar transaction. QRIS's real-time operation and continuously available reporting channels support an expectation of prompt action. Nevertheless, these characteristics do not establish that every delay exceeding 24 hours constitutes negligence. The proposed period functions as a clear protective benchmark. Comparatively, Article 69 of Directive (EU) 2015/2366 requires notification without undue delay, while Article 73 ordinarily requires reimbursement immediately or by the end of the following business day. The latter concerns the provider's reimbursement obligation and should not be presented as a statutory 24-hour reporting rule.

The second tier permits consumer liability of up to 10 per cent of proven preventable additional loss where notification occurs after 24 hours but within three calendar days. This period supplies a limited two-day margin beyond the

initial protective window, accommodating short practical impediments while maintaining an incentive for early reporting. Regulation E provides a useful functional comparison because notification within two business days after learning of the loss or theft of an access device generally attracts a lower liability limit. The proposed three-calendar-day period adopts a different counting method suited to continuously available reporting channels. Its justification therefore depends on accessible notification facilities, exceptions for justified delay, and proof of preventable additional loss, rather than numerical equivalence with the United States rule.

The third tier permits liability of up to 25 per cent of proven preventable additional loss where notification occurs after three but within seven calendar days. The seven-day boundary distinguishes a short reporting delay from an unexplained failure to notify extending across a full week. Its normative purpose is to strengthen the incentive to act without immediately exposing the consumer to the highest proposed liability ceiling. Neither Regulation E nor PSD2 prescribes this seven-day reporting tier. It is an intermediate policy benchmark whose application remains conditional upon demonstrated fault and causation. Reporting during this period should not automatically establish gross negligence, and the PJP must identify the particular losses that earlier notification would have prevented.

The fourth tier permits liability of up to 50 per cent of proven preventable additional loss where notification occurs after seven but within 60 calendar days. The longer window preserves partial consumer protection despite sustained delay while allowing a higher ceiling where that delay demonstrably enables further loss. Regulation E provides a comparative basis for considering a 60-day period, but its period runs from transmission of the relevant periodic

statement. PSD2 instead combines notification without undue delay with an outer notification limit generally extending to 13 months from the debit date. The present model's 60-day period from awareness is therefore an expressly proposed adaptation, requiring its own proportionality justification. Expiry should not automatically extinguish statutory remedies, transfer the initial loss to the consumer, or impose responsibility for losses unrelated to the delay.

The proposed ceilings of 10, 25, and 50 per cent differentiate limited, intermediate, and sustained reporting delay while preserving substantial provider responsibility. They are proposed allocations rather than percentages established by comparative legislation or empirical findings. Their proportionality depends on applying them only to additional losses proven to have been preventable, determining the actual allocation below each ceiling according to fault and causal contribution, and supplementing percentage limits with a maximum nominal amount. For example, if an initial loss of IDR 1,000,000 is followed by IDR 600,000 in proven preventable additional loss, the third-tier ceiling would permit allocation of no more than IDR 150,000 to the consumer because of reporting delay. It would not justify applying 25 per cent to the entire loss. The proposed figures should remain open to regulatory calibration using transaction values, documented loss patterns, reporting accessibility, and the effectiveness of providers' preventive measures.

For clarity, the proposed allocation of liability between consumers and PJPs according to the notification period, the consumer's percentage of liability, and the PJP's reimbursement obligation under the *Time-Bound Tiered Liability Doctrine* is summarised in the following table.

Table 1. Model for the Allocation of Liability under the Time-Bound Tiered Liability Doctrine

Tier	Consumer Notification Period	Consumer Liability	PJP Reimbursement Obligation	Evidentiary Requirement
Tier I	Within 24 hours after the consumer knew or reasonably ought to have known of the unauthorized transaction	0%; the consumer bears no loss	The PJP reimburses 100% of the disputed amount	Full reimbursement may be denied only where the PJP proves intentional conduct, collusion, or the consumer's participation in fraud
Tier II	After 24 hours but no later than three business days	Up to 10% of the additional loss proven to have been preventable through timely notification	The PJP reimburses the entire initial loss and at least 90% of the preventable additional loss	The PJP must prove that delayed notification caused the additional loss
Tier III	After three business days but no later than seven calendar days	Up to 25% of the preventable additional loss	The PJP reimburses the entire initial loss and at least 75% of the preventable additional loss	The PJP must prove when the consumer received notice, when the consumer ought to have known of the transaction, and the causal relationship between the delay and the additional loss
Tier IV	After seven days but within 60 days after the account statement or transaction history became available to the consumer	Up to 50% of the preventable additional loss	The PJP reimburses the entire initial loss and at least 50% of the preventable additional loss	Liability may be allocated to the consumer only where the PJP proves that the additional loss would not have occurred had timely notice been given
After the final deadline	More than 60 days after the account statement or transaction history became available	The consumer may bear all subsequent losses incurred after the expiry of the 60-day	The PJP remains responsible for the initial loss and any loss caused by weaknesses in its system	The PJP must prove that the subsequent loss could have been prevented had the consumer provided notice within the prescribed period

Tier	Consumer Notification Period	Consumer Liability period	PJP Reimbursement Obligation	Evidentiary Requirement
------	------------------------------	---------------------------	------------------------------	-------------------------

Source: Authors' analysis.

The graduated tiers should not apply where delayed notification is supported by a justifiable reason. Such reasons may include the failure to receive a notification, a system disruption, an unavailable reporting channel, hospitalisation, disability, advanced age, force majeure, coercion, or another circumstance that genuinely prevented the consumer from reporting. In those circumstances, the notification period should be extended for a reasonable time. This qualification prevents the reporting deadline from becoming a formal ground for rejecting complaints without regard to the consumer's circumstances.

The doctrine should also regulate provisional reimbursement. The PJP that maintains the consumer's funding source or issues the payment access should bear the first-instance obligation to restore the funds. A consumer should not be required to determine beforehand whether the failure originated with the issuer, acquirer, merchant, switching institution, or technology provider. The allocation of responsibility among the participating entities may be settled subsequently through an inter-party recourse mechanism without delaying restoration of the consumer's rights.

For reports submitted within 24 hours, provisional funds should be restored no later than the end of the following business day after the report and basic information have been received. For reports falling within the second and third tiers, the PJP may be allowed an initial assessment period of no more than three to five business days before granting provisional credit. The final

investigation may continue within the prevailing twenty-business-day complaint-resolution period. If the investigation is not completed within that period, the consumer should remain entitled to use the provisional funds until a final determination is issued.

Provisional reimbursement does not deprive the PJP of its right to investigate. Where the investigation establishes that the transaction was performed by the consumer, conferred a benefit upon the consumer, or involved intentional conduct or fraud, the PJP may reverse the provisional credit. Any reversal must be preceded by written notice stating the reasons, the evidence relied upon, the calculation of the amount to be recovered, and the available mechanism for objection.

For evidentiary purposes, the consumer should be required only to report that the transaction was neither performed nor authorised by the consumer, identify the disputed transaction, and provide information reasonably within the consumer's possession. The PJP should then bear the burden of proving the validity of the authentication, the integrity of the system, the time and device used, receipt of the notification, the results of the fraud assessment, and the presence or absence of consumer fault. The use of a PIN, biometric verification, or a one-time password should constitute only one item of evidence and should not be treated as conclusive proof of the consumer's consent.

Consumers, for their part, should be required to preserve the confidentiality of their credentials, secure their devices, review notifications with reasonable care, report unrecognised transactions promptly, and cooperate with the investigation. A breach of these duties should reduce reimbursement only where the PJP proves a direct causal connection between the breach and the loss. Ordinary negligence should not be equated with gross negligence or

intentional conduct.

As to the form of regulation, the substantive elements of the doctrine should be prescribed in a Bank Indonesia Regulation (*Peraturan Bank Indonesia* or PBI) because they concern consumer rights, PJP obligations, the allocation and limits of liability, the burden of proof, and sanctions. Bank Indonesia Regulation Number 10 of 2025 already places governance, risk management, industry conduct, and consumer protection within the regulation of the payment-system industry. Its regulatory scope provides an appropriate foundation for specific rules governing unauthorized payment transactions.

Once the Bank Indonesia framework has been adopted, banks and non-bank PJPs should be required to implement it through internal policies. The suggested nomenclature is a Policy on the Handling of Unauthorized Payment Transactions and Consumer Reimbursement (*Kebijakan Penanganan Transaksi Pembayaran Tidak Sah dan Pengembalian Dana Konsumen*), supported by detailed standard operating procedures. The policy should allocate responsibilities among the consumer-service, fraud, information-technology, legal, and risk-management functions.

The internal policy should also provide for a 24-hour reporting system, a single complaint-reference number, the freezing of accounts or access devices, the preservation of electronic records, transaction-pattern analysis, provisional reimbursement, and notification of the investigation outcome. Internal policies may not reduce consumer rights, extend regulatory deadlines, increase the consumer's share of liability, or impose requirements not authorised by Bank Indonesia regulations. Their function is to implement the minimum standards prescribed by the regulator, not to replace them.

The Time-Bound Tiered Liability Doctrine therefore treats time as a basis

for allocating liability without making it the sole criterion. The timing of notification must be assessed together with fault, causation, the capacity to prevent loss, and the consumer's circumstances. A consumer who acts promptly should receive full reimbursement, whereas a consumer who delays notification without justification may bear part of the additional loss that could have been prevented. At the same time, the PJP must remain responsible for system weaknesses, authentication failures, undelivered notifications, and other risks within its control. The model provides certainty as to when notice must be given, when funds must be restored, what portion of loss may be allocated to the consumer, and what evidence the PJP must produce. In this manner, consumer protection and provider protection may be balanced in accordance with proportional justice.

4. Conclusion

The study finds that Indonesia's existing legal framework already provides a basis for liability and compensation concerning unauthorized QRIS transactions through electronic-system law, consumer-protection law, and payment-system regulation. These rules establish obligations concerning system security, protection of consumer assets, complaint handling, and compensation for losses attributable to provider fault. In particular, Article 47 of Bank Indonesia Regulation Number 6 of 2026 places the evidentiary burden on the provider, permits exemption where consumer fault is proven, and recognises shared responsibility where both parties are at fault. Nevertheless, the framework does not expressly translate these general responsibility rules into a dedicated mechanism connecting notification timing, quantified consumer liability, preventable additional loss, and substantive reimbursement obligations for unauthorized QRIS transactions. The principal

regulatory gap therefore concerns the operational allocation of losses and restoration of disputed funds, while existing duties, evidentiary requirements, and complaint-handling periods remain applicable.

As a policy reform, this study proposes incorporating the Time-Bound Tiered Liability Doctrine into Indonesia's payment-system regulation. The proposed model uses four reporting intervals: within 24 hours; after 24 hours up to three calendar days; after three up to seven calendar days; and after seven up to 60 calendar days, calculated from when the consumer knew or reasonably ought to have known of the unauthorized transaction. Prompt reporting should attract full reimbursement, subject to proven fraud or intentional misconduct. The subsequent tiers would permit consumer liability of up to 10, 25, and 50 per cent, respectively, confined to additional losses the provider proves resulted from unjustified reporting delay and could have been prevented through timely notification. Initial losses should not be transferred merely because notification was delayed, and expiry of 60 days should not automatically extinguish statutory remedies. The model should also establish provisional reimbursement obligations, reasonable extensions for justified delays, and provider responsibility for losses caused by failure to act after effective notification. Its substantive provisions should be enacted through a Bank Indonesia Regulation, harmonised with existing legislation, supported by implementing regulations, and incorporated into provider policies and procedures. The proposed periods and liability ceilings remain normative recommendations requiring regulatory calibration. Their contribution is to make existing responsibility rules more predictable while advancing legal certainty, proportional justice, and consistent consumer redress.

References

- Agustin, S. L., Fitri, A., Siswanto, F., & Alpiansyah, F. (2025). Kesadaran Keamanan Konsumen dalam Penggunaan Transaksi Digital QRIS sebagai Perlindungan Konsumen Digital: Studi Kasus Penipuan QRIS pada Pedagang Pakaian di Kecamatan Kibin, Kabupaten Serang. *Ar-Rasyid: Jurnal Publikasi Penelitian Ilmiah*, 1(6), 797–805. <https://doi.org/10.64788/AR-RASYID.V1I6.218>
- Aurora, M., Frechette, E., Roth, A., Escobar, L., Zur, O., & Marcella-Burdett, J. (2026). Leading with confidence: QRIS participation and site leaders' confidence, well-being, and quality improvement. *Early Childhood Research Quarterly*, 77, 38–51. <https://doi.org/10.1016/J.ECRESQ.2026.06.004>
- Ayuningtyas, A., Adinugraha, H. H., & Sulthoni, M. (2024). Quick Response Code Indonesian Standard as a Digital Payment Solution to Increase the Turnover and Reduce the Circulation of Counterfeit Money. *Journal of Education and Computer Applications*, 1(1), 25–31. <https://doi.org/10.69693/JECA.V1I1.7>
- Budnitz, M. E. (2025). Big Tech and Consumer Payments: The Good, the Bad, and the Unintended Consequences. *Loyola Consumer Law Review*, 37. <https://access.heinonline.com/HOL/Page?handle=hein.journals/lyclr37&id=134&div=&collection=>
- Callaway, L. (2022). When an un-submitted stop-payment request still matters to banks. *Banking Journal*, 115.
- Hamka, N. M., Nopiya, S., Pebyani, T., Fitriani, S., Limbong, V., & Yulianah, Y. (2026). Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia. *Advances in Community Services Research*, 4(2), 68–81. <https://doi.org/10.60079/ACSR.V4I2.878>
- Hamzah Muchtar, E., Trianto, B., Maulana, I., Alim, M. N., Marasabessy, R. H., Hidayat, W., Junaedi, E., & Masrizal. (2024a). Quick response code Indonesia standard (QRIS) E-payment adoption: customers perspective. *Cogent Business & Management*, 11(1), 1–18. <https://doi.org/10.1080/23311975.2024.2316044>
- Hamzah Muchtar, E., Trianto, B., Maulana, I., Alim, M. N., Marasabessy, R. H., Hidayat, W., Junaedi, E., & Masrizal. (2024b). Quick response code Indonesia standard (QRIS) E-payment adoption: customers perspective. *Cogent Business and Management*, 11(1). <https://doi.org/10.1080/23311975.2024.2316044>
- Khadapi, Moh. A., Hamzani, A. I., & Wildan, M. (2023). Tinjauan Hukum Pencegahan Konflik Dalam Pembagian Waris Menurut Hukum Perdata. *Jurnal Studi Islam Indonesia (JSII)*, 1(1), 33–50. <https://doi.org/10.61930/JSII.V1I1.129>
- Kierner, T., Middlebrook, S. T., & Hughes, S. J. (2026). "Spinning Wheel Got to Go Round": Developments in the Law Affecting Electronic Payments and Financial Services.

- Business Lawyer*, 81(1), 333–344. <https://doi.org/10.2139/SSRN.6556323>
- Marianingsih, I., Salim, & Mijinyawa, S. I. (2026). Aligning Sharia Contracts and Payment Regulation: An Operational Governance Framework for Electronic Money in Indonesia. *Journal of Islamic Economic and Business Research*, 6(1), 145–158. <https://doi.org/10.18196/JIEBR.V6I1.477>
- Matthew Jakaria Sitanggang, & Imam Haryanto. (2025). QRIS as a Single Payment Gateway as a Solution for Payment Efficiency and Legal Protection for e-commerce Consumers Through a Comparison With China. *Journal of Law, Politic and Humanities*, 5(3), 1840–1852. <https://doi.org/10.38035/JLPH.V5I3.1339>
- Mulia, W. D., & Bangsawan, Moh. I. (2025). Legal Protection against BRI's Quick Response Code Indonesian Standard (QRIS) Transactions in Micro, Small, and Medium Enterprises in Kartasura District. *Proceeding International Conference Restructuring and Transforming Law*, 4(1), 501–513. <https://proceedings.ums.ac.id/icrtlaw/article/view/5762>
- Mumtakhinah, R. I., Triandani, S., Noor, N. A., Apriliani, R. F., Ramadhani, B. I. C., & Baidhowi. (2026). Surcharge dalam Transaksi QRIS: Analisis Perlindungan Konsumen dan Penegakan Hukum Berdasarkan Peraturan Bank Indonesia. *Sinergi: Jurnal Ilmiah Multidisiplin*, 2(6), 2844–2865. <https://doi.org/10.66914/289BX057>
- Patterson, J. A. (2022). Innovating to Fight Fraud: Potential Approaches to the Problem of Unauthorized Transfers under Regulation E. *Consumer Finance Law Quarterly Report*, 76. <https://access.heinonline.com/HOL/Page?handle=hein.journals/cnsmrfinlw76&id=283&div=&collection=>
- Pattynama, F. M., Santoso, H. A., Rachmad, F., Miarsa, D., Pribadi, T., Maarif, U., & Latif, H. (2024). LEGAL PROBLEMS FOR QUICK RESPONSE CODE INDONESIAN STANDARD (QRIS) USERS IN ONLINE PAYMENT TRANSACTIONS. *ANAYASA: Journal of Legal Studies*, 2(1), 44–55. <https://doi.org/10.61397/AYS.V2I1.183>
- Purwanto, K., Mulyani, A., & Ferdinal, A. (2025). The Influence of Public Perception, Trust, and Lifestyle on Interest in Using QRIS in Transactions at the Cahaya USA Store. *JIMU (JURNAL ILMIAH MANAJEMEN UBHARA)*, 7(2), 69–75. <https://doi.org/10.31599/NSNTDG56>
- Ramah, G. N., Saliman, A. R., & Dewi, V. (2024). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Non Tunai Yang Menggunakan Qris (Studi Lapangan Bank Rakyat Indonesia Cabang Pangkalpinang). *UNES Law Review*, 7(2), 823–831. <https://doi.org/10.31933/UNESREV.V7I2.2367>
- Sanchez-Adams, C. (2024). Scams, Deception and Fraud in the Banking System: Potential Remedies for Consumers. *Journal of Consumer & Commercial Law*, 28. <https://access.heinonline.com/HOL/Page?handle=hein.journals/jlocncllw28&id=76&div=&collection=>

- Saraswati, I. S., Suparwi, S., & Zaelani, M. A. (2026). Perlindungan Hukum Konsumen dalam Transaksi QRIS Berdasarkan Regulasi Bank Indonesia: Consumer Legal Protection in QRIS Transactions Under Bank Indonesia Regulations. *Semarang Law Review (SLR)*, 7(1), 289–306. <https://doi.org/10.26623/SLR.V7I1.13980>
- Sasra, A. D., & Baidhowi, B. (2025). PERLINDUNGAN HUKUM DALAM TRANSAKSI NONTUNAI BERBASIS QUICK RESPONSE CODE INDONESIAN STANDARDS (QRIS) BERDASARKAN PERSPEKTIF HUKUM PERBANKAN. *JURNAL ILMIAH NUSANTARA*, 2(4), 266–274. <https://doi.org/10.61722/JINU.V2I4.5030>
- Satriatama, R., & Dikrurahman, D. (2026). Pertanggungjawaban Hukum Merchant QRIS terhadap Kerugian Konsumen Akibat Kegagalan Settlement. *Jurnal Hukum Lex Generalis*, 7(4). <https://doi.org/10.56370/JHLG.V7I4.3687>
- Selznick, L. F., & LaMacchia, C. (2015). Cybersecurity: Should the SEC Be Sticking Its Nose Under This Tent? *Journal of Law, Technology and Policy*, 1(1). https://doi.org/10.1163/1872-9037_AFCO_ASC_3264
- Sitanggang, M. J., & Haryanto, I. (2025). QRIS as a Single Payment Gateway as a Solution for Payment Efficiency and Legal Protection for e-commerce Consumers Through a Comparison With China. *Journal of Law, Politic and Humanities*, 5(3), 1840–1852. <https://doi.org/10.38035/JLPH.V5I3.1339>
- Subihana Putri, P., Adlina, H., & Utara Abstrak, S. (2025). Pengaruh Persepsi Kemudahan Dan Persepsi Manfaat Dalam Penggunaan Qris Terhadap Efisiensi Penggunaan Dompot Digital Ovo Pada Masyarakat Kota Medan. *Jurnal Ilmiah Wahana Pendidikan*, 11(4.D), 124–134. <https://jurnal.peneliti.net/index.php/JIWP/article/view/10215>
- Syahrin, K., Arisandy, Y., & Handika, Y. (2025). The Influence of Convenience, Benefits, and Security on Consumer Preferences in Adopting QRIS Non-Cash Payments. *Airlangga Journal of Innovation Management*, 6(3), 521–541. <https://doi.org/10.20473/ajim.v6i3.77544>
- Tara, I. K. K. B., & Sudiro, A. (2023a). Perlindungan Hukum Konsumen Terhadap Pengguna Qris dan Penanganan Penipuan dalam Bertransaksi. *UNES Law Review*, 6(2), 4581–4588. <https://doi.org/10.31933/UNESREV.V6I2.1498>
- Tara, I. K. K. B., & Sudiro, A. (2023b). Perlindungan Hukum Konsumen Terhadap Pengguna Qris dan Penanganan Penipuan dalam Bertransaksi. *UNES Law Review*, 6(2), 4581–4588. <https://doi.org/10.31933/UNESREV.V6I2.1498>
- Wicaksono, D. T., Rahman, Prasetya, F., Lestari, N. P., & Diar, A. (2026). Efektivitas Undang-Undang No. 7 Tahun 2011 Tentang Mata Uang Terhadap Pembayaran Non Tunai: Studi Kasus: Roti'O Halte Transjakarta Monas. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, 4(2), 2973–2988. <https://doi.org/10.61104/ALZ.V4I2.4822>
- Yana, M., Arief, A., & Rahim, D. (2026). QRIS and Digital Consumer Protection: A Forensic Legal Study of the Risks of Data Misuse and Electronic Disputes. *INDONESIA LEGAL ADVANCED JOURNAL*, 1(2).

<https://inled.journal.umi.ac.id/index.php/inled/article/view/21>

Zulia Ramdhani, F., Hashfi Luthfi, A., & Sunan Kalijaga, U. (2025). Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation. *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum*, 59(2), 191–213. <https://doi.org/10.14421/AJISH.V59I2.1594>