Volume 12 Issue 2, 2026
P-ISSN: 2442-8019, E-ISSN: 2620-9837
DOI: 10.55809/tora.v12i2.746

Article history: Received January 31, 2026; Accepted May 13, 2026; Available online June 25, 2026

IMPLEMENTATION OF BANK INDONESIA REGULATION NUMBER 2 OF 2024 IN STRENGTHENING CONSUMER PROTECTION AT THE BANK INDONESIA REPRESENTATIVE OFFICE IN CENTRAL JAVA PROVINCE

Suciyaningsih[1], Adi Suliantoro[2]

[1] Fakultas Hukum, Universitas Stikubank Semarang, Indonesia. E-Mail: Suciyaningsih2511@gmail.com
[2] Fakultas Hukum, Universitas Stikubank Semarang, Indonesia. E-Mail: adisuliantoro@edu.unisbank.ac.id

Abstract: *This empirical juridical study examines the implementation of Bank Indonesia Regulation Number 2 of 2024 on information system security and cyber resilience as a framework for strengthening consumer protection at the Bank Indonesia Representative Office in Central Java Province. The expansion of QRIS, BI-FAST, electronic wallets, mobile banking, and other digital payment services has improved transaction efficiency while increasing exposure to system disruptions, personal data misuse, phishing, account takeover, and social engineering. The study used a descriptive-analytical design. Primary data were obtained through interviews and observations at the Bank Indonesia Representative Office in Central Java Province between December 2025 and February 2026, while secondary data consisted of legislation, regulatory documents, institutional reports, books, and peer-reviewed literature. The data were analyzed qualitatively by relating the applicable legal framework to empirical implementation. The findings show that the regulation has shifted protection toward preventive, risk-based supervision through governance, identification, protection, detection, response, recovery, reporting, and inter-agency coordination. Nevertheless, implementation is constrained by centralized supervisory authority, uneven technological and human-resource capacity among payment service providers, incomplete incident reporting, and low consumer digital-security literacy. The study concludes that the regulation provides a strong legal basis, but its effectiveness depends on coordinated supervision, provider compliance, interoperable incident handling, and sustained public education. The article also notes the issuance of Bank Indonesia Regulation Number 6 of 2026 after data collection as a subsequent development in the consumer-protection framework.*

Keywords: *Bank Indonesia; consumer protection; cyber resilience; digital payment systems; information system security.*

How to Site: Suciyaningsih, Suliantoro, A. (2026). Implementation of Bank Indonesia Regulation Number 2 of 2024 in Strengthening Consumer Protection at the Bank Indonesia Representative Office in Central Java Province. *Jurnal Hukum to-ra: Hukum untuk mengatur dan melindungi masyarakat*, 12 (2), pp 256-271.

Introduction

Digitalization has transformed the Indonesian payment system by enabling consumers to conduct transactions through mobile banking, internet banking, electronic money, electronic wallets, QRIS, BI-FAST, and other financial-technology platforms. This development has widened access and accelerated payment activity, but it has also

increased dependence on interconnected information systems. Bank Indonesia reported continued growth in digital payment activity throughout 2024, supported by wider acceptance of QRIS and the development of national payment infrastructure (Bank Indonesia, 2025a, 2025b, 2025c). Consequently, the reliability and security of digital payment systems have become integral to both financial-system stability and the protection of consumer rights.

The expansion of digital services creates risks that differ from those associated with conventional transactions. System downtime, pending transactions, malware, credential theft, account takeover, manipulation of QR codes, phishing, and unauthorized use of personal data may cause direct financial loss and undermine public confidence. Phishing and social-engineering attacks are particularly difficult to prevent because they combine technological methods with manipulation of trust, urgency, fear, and authority. Research consistently shows that technical safeguards alone are insufficient when users cannot distinguish legitimate communications from deceptive ones (Alkhalil et al., 2021; Desolda et al., 2022; Naqvi et al., 2023; Sarno & Black, 2024; Zhuo et al., 2023).

From a legal perspective, consumer security in digital finance is protected through several complementary instruments. Law Number 8 of 1999 recognizes the consumer's right to comfort, security, and safety. Law Number 27 of 2022 regulates the processing and protection of personal data, while Law Number 1 of 2024 strengthens the legal framework for electronic information and transactions. Law Number 4 of 2023 further reinforces the authority of financial-sector regulators, including Bank Indonesia, in technology governance, consumer protection, and financial-sector resilience (Republic of Indonesia, 1999, 2022, 2023, 2024). These provisions require consumer protection to be understood not merely as post-loss compensation but also as prevention, secure system design, effective supervision, and accessible dispute resolution.

Within this framework, Bank Indonesia Regulation Number 2 of 2024 on Information System Security and Cyber Resilience requires regulated entities to establish governance, prevention, detection, response, recovery, reporting, and collaboration mechanisms. Its operational requirements are elaborated in Regulation of the Members of the Board of Governors Number 24 of 2024. During the research period, consumer protection was also governed by Bank Indonesia Regulation Number 3 of 2023 and Regulation of the Members of the Board of Governors Number 20 of 2023, together with Bank Indonesia Regulation Number 3 of 2024 on the Financial Sector Alternative Dispute Resolution Institution (Bank Indonesia, 2023a, 2023b, 2024a, 2024b, 2024c). The combined framework places cybersecurity, data protection, information disclosure, complaint handling, and business conduct within a unified supervisory environment.

The urgency of effective implementation is also reflected in the increasing institutional response to financial scams. The Indonesia Anti-Scam Centre has demonstrated the importance of rapid coordination among regulators, banks, payment providers, telecommunications operators, and law-enforcement agencies to trace and suspend fraudulent transactions (Financial System Stability Committee, 2026). At the regional level, however, detailed public data remain limited, while complaints are often handled through different institutional channels. This situation makes regional empirical research important because the effectiveness of national regulation ultimately depends on institutional capacity, supervisory coordination, provider compliance, and consumer behavior in specific local contexts.

Previous studies have discussed consumer protection in fintech transactions, the role of the Financial Services Authority, and the relationship between regulation, supervision, data protection, and fraud prevention (Arifin et al., 2023; Pratiwi et al., 2022). International frameworks likewise emphasize governance, operational resilience, fair treatment, data protection, disclosure, financial education, and effective complaint mechanisms (Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, 2016; National Institute of Standards and Technology, 2024; OECD, 2022). Nevertheless, limited research has examined how Bank Indonesia Regulation Number 2 of 2024 is implemented by a regional representative office and how administrative, technical, and literacy-related constraints influence consumer protection.

Accordingly, this study addresses three questions: (1) what forms of digital-finance security risk are encountered in protecting consumers in Central Java; (2) how is Bank Indonesia Regulation Number 2 of 2024 implemented by the Bank Indonesia Representative Office in Central Java Province; and (3) what obstacles affect implementation at the regional level? The study aims to evaluate the practical operation of the regulation and to identify measures required to strengthen preventive and remedial consumer protection in the digital payment system.

A regulatory development occurred after completion of the fieldwork. Bank Indonesia Regulation Number 6 of 2026 on Bank Indonesia Consumer Protection was issued in June 2026 and replaced Bank Indonesia Regulation Number 3 of 2023. Because the interviews and observations in this study were completed in February 2026, the new regulation is treated as a subsequent legal development rather than as part of the empirical implementation assessed. Its inclusion ensures that the article reflects the legal position at the publication stage without altering the study's focus on Bank Indonesia Regulation Number 2 of 2024 (Bank Indonesia, 2026).

Method

This study employed an empirical juridical approach with a descriptive-analytical design. Empirical juridical research examines the operation of legal norms by connecting documentary legal analysis with facts obtained from the field (Muhammad, 2004). The approach was selected because the object of inquiry was not limited to the content of Bank Indonesia Regulation Number 2 of 2024, but also included its implementation through supervision, incident handling, consumer education, complaint services, and institutional coordination in Central Java.

Primary data were obtained from interviews and observations at the Bank Indonesia Representative Office in Central Java Province. The field materials included an interview with the payment-system policy implementation function on 30 December 2025; interviews concerning supervision, legal protection, and policy implementation on 9 and 12 February 2026; and an observation of the payment-system policy implementation unit on 11 February 2026. Informants were selected purposively on the basis of their institutional duties and knowledge of payment-system supervision, cybersecurity risk, and consumer protection. The article reports institutional findings rather than attributing policy statements to individual employees.

Secondary data were collected through a review of primary legal materials, including statutes, Bank Indonesia regulations, implementing regulations, and related Financial Services Authority provisions. Secondary legal materials consisted of books, peer-reviewed journal articles, institutional reports, international standards, and relevant policy documents. The legal materials were used to interpret the scope of regulatory obligations, while the academic literature was used to assess the consistency of the empirical findings with research on phishing, digital financial literacy, cyber resilience, and consumer protection.

The data were analyzed qualitatively through four stages: data reduction, thematic classification, comparison between legal requirements and field implementation, and deductive interpretation. The themes were organized around digital-security risk, regulatory implementation, and implementation barriers. Source triangulation was conducted by comparing interview statements, observation notes, regulatory provisions, and documentary evidence. The study is limited to the institutional perspective of one Bank Indonesia representative office and does not measure the compliance of each payment service provider individually; therefore, the conclusions concern implementation patterns and constraints rather than a statistical assessment of national regulatory effectiveness.

Results and Discussion

Digital-Finance Security Risks in Consumer Protection

The findings indicate that consumer risk in Central Java arises from an interaction between technical failure, cyberattack, misuse of personal data, and user vulnerability. Technical risks include system downtime, delayed transaction confirmation, interrupted services, inadequate server capacity, weaknesses in access control, and insufficient recovery arrangements. A failed or pending transaction may create legal uncertainty when the consumer's balance has been debited but the payment is not immediately confirmed. Under Bank Indonesia Regulation Number 2 of 2024, these risks must be addressed through governance, risk identification, system protection, monitoring, incident response, service recovery, and continuous improvement (Bank Indonesia, 2024a, 2024b).

Operational continuity is therefore a component of consumer protection rather than a purely technical matter. The international cyber-resilience framework for financial-market infrastructures similarly treats preparedness, response, recovery, and learning as an integrated cycle, while the NIST Cybersecurity Framework 2.0 organizes risk management through govern, identify, protect, detect, respond, and recover functions (Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, 2016; National Institute of Standards and Technology, 2024). The field findings are consistent with these frameworks: protection is effective only when a provider can prevent disruption, identify an incident promptly, communicate with affected users, restore service, and correct the underlying weakness.

A second and prominent risk is social engineering. Fraudsters increasingly exploit psychological rather than technical vulnerabilities through phishing links, fraudulent calls, fake customer-service accounts, requests for one-time passwords, and manipulated payment codes. The consumer may voluntarily disclose credentials because the message appears urgent or originates from a seemingly legitimate institution. Systematic reviews show that low security awareness, habitual responses, overreliance on authority cues, and limited capacity to evaluate digital messages increase phishing susceptibility (Alkhalil et al., 2021; Desolda et al., 2022; Naqvi et al., 2023; Zhuo et al., 2023). The empirical findings therefore support the view that cybersecurity controls must be complemented by behavioral education and clear risk communication.

Digital literacy is closely related to this vulnerability. Consumers who understand financial products but lack digital-security competence may still be unable to identify fake applications, malicious links, excessive access permissions, or suspicious requests for credentials. Research on digital financial literacy emphasizes that consumers require both financial capability and the ability to recognize technology-related risks

(Koskelainen et al., 2023; Panos & Wilson, 2020). Sarno and Black (2024) further found that lower digital literacy and lower cognitive reflection were associated with poorer discrimination between legitimate and deceptive messages. These findings explain why public education is a substantive protective measure, not merely a supplementary promotional activity.

A third risk concerns personal data and identity misuse. Population identification numbers, telephone numbers, account credentials, biometric information, and transaction histories can be used to take over accounts, initiate unauthorized transactions, or submit unlawful credit applications. Law Number 27 of 2022 requires personal-data controllers to ensure lawful processing and data security, while Bank Indonesia Regulation Number 2 of 2024 requires regulated entities to protect the confidentiality, integrity, and availability of information (Republic of Indonesia, 2022; Bank Indonesia, 2024a). Consumer harm in such cases may extend beyond the initial financial loss because the victim must also restore control over the account and identity.

The allocation of responsibility creates a further legal issue. Providers may attribute the loss to consumer negligence, whereas consumers often lack access to system logs or the technical expertise required to prove a provider-side weakness. This evidentiary imbalance can delay reimbursement and complaint resolution. The principles of fair treatment, transparency, responsible business conduct, and effective redress require providers to conduct a traceable investigation and explain the basis of their decision (OECD, 2022; Financial Services Authority, 2023). Accordingly, incident investigation should not rely on a binary distinction between “system failure” and “consumer fault,” but should assess whether authentication, fraud monitoring, warning messages, transaction limits, and response procedures were proportionate to the foreseeable risk. Figure 1 maps the relationship between the digital services supervised by Bank Indonesia and the principal security risks identified in the study.

Forms of Digital-Finance Services and Principal Consumer-Security Risks

Supervisory object	Service examples	Principal risks
Payment system	BI-FAST, QRIS, debit cards	Transaction disruption; QR-code manipulation; credential theft; false confirmation
Payment service provider (PJP)	Electronic wallets, payment gateways, fund transfers	Account takeover; customer-profile leakage; unauthorized transfers; balance loss
Digital banking services	Mobile banking and internet banking	Phishing; malware; interception of PIN or OTP; fake applications and websites
Payment-system infrastructure	Payment-system infrastructure provider (PIP)	Ransomware; unauthorized database access; server failure; prolonged service interruption

Risk profiles differ by service architecture, interconnection, transaction exposure, and user behavior; supervision should therefore be proportional and risk-based.

Figure 1. Relationship between Bank Indonesia's supervisory objects and digital-finance security risks.

Source: Adapted from Bank Indonesia Regulation Number 2 of 2024 and processed field data (2026).

The mapping demonstrates that each payment channel has a distinct risk profile. Mobile and internet banking are vulnerable to credential theft, malware, and account takeover; QRIS and fund-transfer services may be affected by code manipulation, transaction failure, or false confirmation; electronic wallets and payment gateways are exposed to identity misuse and unauthorized access; and payment-system infrastructure may be targeted by ransomware or service-disruption attacks. The regulatory response must therefore be risk-based rather than uniform. Providers with greater interconnection, transaction volume, and systemic relevance require stronger governance, testing, monitoring, and recovery capacity.

The findings also reveal a digitalization paradox. QRIS, BI-FAST, and electronic wallets improve efficiency and financial inclusion, but rapid adoption may precede the development of secure consumer habits. Cybercriminals can therefore bypass strong institutional encryption by manipulating the user. Effective protection requires a balance among three pillars: adaptive regulation and supervision by Bank Indonesia, technological and procedural compliance by payment service providers, and informed vigilance by consumers. Weakness in any one pillar reduces the effectiveness of the other two.

Implementation of Bank Indonesia Regulation Number 2 of 2024

The first implementation finding is a shift from reactive protection toward preventive cyber-risk governance. Before a consumer suffers a loss, a Payment Service Provider (Penyelenggara Jasa Pembayaran, PJP) is expected to identify critical assets, assess

threats and vulnerabilities, establish internal responsibilities, protect systems and data, detect anomalies, and prepare response and recovery plans. This structure is consistent with the preventive conception of legal protection, in which rights are safeguarded through administrative controls before a dispute occurs (Hadjon, 1987). It also reflects the broader international movement from compliance-based security toward operational resilience (Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, 2016).

At the governance level, implementation begins with the allocation of responsibility within the provider, the preparation of strategic plans, security policies, standards, procedures, and an organizational function responsible for information-system security and cyber resilience. Regulation of the Members of the Board of Governors Number 24 of 2024 differentiates implementation according to the provider's service characteristics and system interconnection. This proportional approach is important because a provider directly connected to Bank Indonesia or other critical infrastructure presents a different risk from an entity that only uses stand-alone or client systems (Bank Indonesia, 2024b).

At the licensing and supervisory stages, Bank Indonesia evaluates the provider's technological readiness, information-security policies, data-protection controls, internal governance, and human-resource capacity. Supervision is then continued through periodic reporting, security testing, information-technology audits, incident reporting, on-site examination, and off-site risk analysis. The field findings indicate that reports and incident data are used to map provider risk and determine supervisory priorities. This approach allows Bank Indonesia to concentrate resources on providers whose services, connectivity, transaction exposure, or prior incidents indicate a higher level of risk.

Cyber resilience is implemented as a guarantee of service continuity. Providers are expected to prepare incident-response and recovery procedures, conduct simulations, maintain backup capacity, restore critical services, and communicate with relevant stakeholders. Consumer protection requires communication to be timely and intelligible: users should know whether a transaction failed, whether funds remain secure, what actions they must take, and how the provider will resolve the incident. A technically successful recovery that leaves consumers without information may still fail to satisfy the principles of transparency and fair treatment.

Protection of personal data is implemented through access restrictions, encryption, authentication, transaction monitoring, logging, and controls over third-party processing. These measures support the requirements of Law Number 27 of 2022 and reduce opportunities for unauthorized account access. However, security design should also consider usability. Excessively complex controls may encourage consumers to adopt unsafe workarounds, whereas weak authentication exposes accounts to takeover. The

appropriate standard is therefore layered and risk-sensitive protection that remains understandable and usable for consumers.

Information disclosure and education form another part of implementation. During the research period, the Bank Indonesia consumer-protection framework required providers to disclose product features, costs, benefits, risks, complaint procedures, and relevant consumer obligations (Bank Indonesia, 2023a, 2023b). The Bank Indonesia Representative Office in Central Java Province also used public-education activities, including the PeKA campaign—Peduli, Kenali, Adukan—to remind consumers to protect PINs, passwords, and one-time passwords, verify communications, and report suspicious activity. Such education is consistent with evidence that repeated, behavior-oriented interventions are more useful than general warnings that do not train consumers to identify attack cues (Koskelainen et al., 2023; Naqvi et al., 2023).

Complaint handling operates as the remedial component of protection. Consumers may submit complaints through provider channels and, where relevant, through Bank Indonesia's consumer-protection function. Unresolved disputes may proceed to the Financial Sector Alternative Dispute Resolution Institution under Bank Indonesia Regulation Number 3 of 2024. The availability of an external dispute-resolution route is important because it reduces the imbalance between individual consumers and service providers and creates an incentive for providers to maintain documented, consistent, and reviewable complaint decisions (Bank Indonesia, 2024c).

The field findings further show that cyber incidents require cross-agency coordination. Bank Indonesia is responsible for payment-system continuity and the entities under its authority; the Financial Services Authority supervises other financial-services institutions and applies sector-wide consumer-protection requirements; the National Cyber and Crypto Agency supports national cyber coordination; and law-enforcement agencies investigate criminal conduct. Cooperation may include information exchange, transaction tracing, account blocking or suspension, technical analysis, and evidence support. Indonesian studies similarly conclude that regulatory coordination, supervision, and data protection are necessary to reduce fraud and prevent overlapping authority (Arifin et al., 2023; Pratiwi et al., 2022).

Overall, Bank Indonesia Regulation Number 2 of 2024 has been implemented as more than a technical security standard. It links system governance to the legal interests of consumers by requiring providers to prevent foreseeable harm, maintain continuity, protect data, report incidents, and participate in supervisory and collaborative mechanisms. Nevertheless, the evidence supports a qualified rather than absolute assessment of effectiveness. The regulation is substantively adequate, but practical effectiveness depends on the quality of reporting, the speed of coordination, provider capacity, enforcement consistency, and consumer ability to respond securely.

Administrative, Technical, and Literacy-Related Barriers

The principal administrative barrier is the division of supervisory authority between the central office and the regional representative office. Many major payment service providers are headquartered in Jakarta. Consequently, findings arising in Central Java may need to be reported to Bank Indonesia's head office before a direct audit, formal supervisory action, or sanction can be taken. This arrangement supports national consistency, but it may lengthen the response to local complaints or emerging incident patterns. The issue is therefore not the absence of authority, but the need for clear escalation thresholds, interoperable case records, and time-bound coordination between central and regional units.

A related barrier concerns the completeness and timeliness of provider reporting. Bank Indonesia Regulation Number 2 of 2024 and its implementing regulation require information relevant to supervision and cyber incidents. The field data indicate that smaller and medium-sized providers may face difficulty preparing reports that meet the expected technical detail and submission timetable. Incomplete reporting weakens risk mapping, delays the identification of repeated incidents, and limits the ability of the regional office to explain the status of a consumer complaint. Standardized incident taxonomies, digital reporting templates, and targeted technical assistance would improve both compliance and supervisory usability.

These administrative findings can be explained through Soekanto's theory of legal effectiveness, which identifies legal substance, law enforcement, facilities, society, and legal culture as interdependent factors (Soekanto, 2018). Bank Indonesia Regulation Number 2 of 2024 provides a clear normative structure, but implementation is influenced by institutional coordination, information quality, supervisory resources, and provider compliance. A strong rule may therefore produce uneven outcomes when the supporting institutional mechanisms are not equally mature.

Technical barriers arise from differences in infrastructure, investment capacity, and cybersecurity expertise among providers. Layered security, continuous monitoring, vulnerability testing, backup facilities, and incident-response capability require sustained expenditure and specialized personnel. Large providers may absorb these requirements more readily than smaller entities. The proportional approach in Regulation of the Members of the Board of Governors Number 24 of 2024 reduces unnecessary uniformity, but proportionality must not be interpreted as permission to provide a level of security that is inadequate for the risk actually created by the service.

The observations also identified transaction delays during periods of high demand and compatibility problems on older consumer devices. These problems should not be simplistically attributed to the security features themselves. They may result from insufficient server capacity, inefficient application design, connectivity limitations, or

failure to optimize an application across devices. The consumer-protection implication is that providers should test both security and usability, communicate service limitations, and provide a prompt mechanism for reconciling transactions when a balance has been debited without immediate confirmation.

Technical and administrative barriers have a direct legal effect. Delayed reporting may slow incident containment, while inadequate infrastructure may increase the probability or duration of disruption. In Hadjon's conception, legal protection is effective only when institutional implementation secures the rights promised by the legal norm (Hadjon, 1987). Accordingly, compliance should be assessed not only through the existence of policies and documents, but also through measurable readiness to prevent, detect, respond to, and recover from incidents.

Consumer literacy is the third major barrier. Table 1 summarizes the complaint classification contained in the study's processed primary and secondary data for 2024–2025.

Table 1. Classification of consumer complaints related to cybersecurity and digital payment systems in Central Java, 2024–2025.

No.	Incident/Complaint Category	Transaction Type	Complaints	Share	Handling Status
1	Social engineering (phishing and OTP fraud)	Mobile banking and e-wallet	145	45%	Education and coordination with the Central Java Regional Police
2	Misuse of personal data	Digital payment accounts	48	15%	Investigation of PJP compliance
3	PJP system failure	QRIS and fund transfer	98	30%	Mediation and refund instruction
4	Malware/digital skimming attacks	Mobile banking	20	6%	Technical audit of the provider's IT system
5	Other complaints	Various	12	4%	Handling according to the complaint type
	Total		**323**	**100%**	

Source: Interviews with the Bank Indonesia Representative Office in Central Java Province and secondary Bank Indonesia data, processed by the authors (2026).

Table 1 indicates that social engineering accounted for 45% of the classified complaints, followed by PJP system failure at 30%. Because the table was compiled from the study's processed data rather than a complete population of all incidents in Central Java, it should be interpreted descriptively. Even so, the pattern reinforces the central finding that consumer vulnerability is not solely an infrastructure problem. Fraudsters often exploit the human decision point after technical defenses have protected the provider's core system.

The relevant behavioral issue is not an assumed cultural characteristic of Central Java residents, but the interaction of trust, urgency, limited verification habits, and unequal access to security education. Messages that imitate institutions, threaten account suspension, or promise rewards can induce consumers to disclose credentials before evaluating authenticity. Contemporary social-engineering research also warns that

generative artificial intelligence can make fraudulent messages more realistic, personalized, and scalable (Schmitt & Flechais, 2024). Education must therefore train consumers to pause, verify through official channels, refuse requests for PINs or one-time passwords, and report suspicious activity promptly.

The reach of education is also uneven. Public campaigns are more visible in large urban centers, while consumers in smaller cities and rural areas may depend on informal information circulated through social media or interpersonal networks. A sustainable literacy strategy should therefore involve local governments, educational institutions, community organizations, telecommunications providers, banks, and payment providers. Digital financial literacy should be incorporated into routine consumer interaction rather than delivered only after a major incident (Koskelainen et al., 2023; Panos & Wilson, 2020).

Product complexity creates an additional communication barrier. Applications increasingly combine payments, transfers, credit, investment, and identity services, but terms and permission requests are often expressed in technical language. Consumers may grant extensive access without understanding the privacy consequence. The principles of disclosure and transparency require information to be accurate, timely, accessible, and comprehensible, not merely present in a lengthy standard agreement (OECD, 2022; Financial Services Authority, 2023).

Low cyber hygiene further increases risk. Shared devices, outdated operating systems, installation of applications from unofficial sources, reuse of passwords, and transactions through insecure networks can expose financial applications to malware or unauthorized access. The appropriate regulatory response is shared responsibility. Providers must implement secure defaults, layered authentication, anomaly detection, and clear warnings; regulators must supervise and coordinate; and consumers must apply basic security practices. Treating every incident as either entirely the provider's fault or entirely the consumer's fault obscures this interdependence.

Taken together, the barriers show that successful implementation requires more than normative compliance. The regional office needs efficient escalation to the central office, providers need sufficient technological and reporting capacity, and consumers need practical security competence. The updated Bank Indonesia consumer-protection framework issued after the fieldwork strengthens the relevance of data protection, risk management, transparency, literacy, complaint handling, and market conduct. Future implementation should therefore integrate Bank Indonesia Regulation Number 2 of 2024 with Bank Indonesia Regulation Number 6 of 2026 while preserving the empirical distinction between the period studied and the law applicable at publication (Bank Indonesia, 2026).

Conclusion

Bank Indonesia Regulation Number 2 of 2024 has provided a coherent legal basis for strengthening consumer protection through information-system security and cyber resilience at the Bank Indonesia Representative Office in Central Java Province. The principal risks identified were technical and operational disruption, personal-data misuse, phishing, account takeover, and social engineering. Implementation has moved protection toward a preventive and risk-based model through governance, licensing assessment, on-site and off-site supervision, reporting, incident response, recovery, public education, complaint handling, and cross-agency coordination. The regulation is therefore relevant not only to system stability but also to the consumer's rights to security, information, fair treatment, and effective redress. Its effectiveness remains conditional on implementation capacity. Centralized authority may delay regional follow-up; smaller providers may face technological, reporting, and human-resource constraints; and uneven digital-security literacy leaves consumers vulnerable to manipulation. Bank Indonesia should strengthen time-bound coordination between central and regional offices, standardize cyber-incident reporting, apply proportional but enforceable technical requirements, and expand behavior-oriented education beyond major urban centers. Providers should combine secure system design with transparent investigation and accessible complaint resolution. The issuance of Bank Indonesia Regulation Number 6 of 2026 after the fieldwork should be incorporated into subsequent supervision and research, while the findings of this study remain an assessment of the implementation environment observed through February 2026.

Reference

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, Article 563060. https://doi.org/10.3389/fcomp.2021.563060

Arifin, Z., Lestari, R. I., Saifudin, & Putrisetia, D. A. (2023). Peran Otoritas Jasa Keuangan dalam pengawasan jasa layanan keuangan berbasis financial technology peer-to-peer lending. Jurnal USM Law Review, 6(2), 712–723. https://doi.org/10.26623/julr.v6i2.7170

Bank Indonesia. (2023a). Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Pelindungan Konsumen Bank Indonesia.

Bank Indonesia. (2023b). Peraturan Anggota Dewan Gubernur Nomor 20 Tahun 2023 tentang Tata Cara Pelaksanaan Pelindungan Konsumen Bank Indonesia.

Bank Indonesia. (2024a). Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia.

Bank Indonesia. (2024b). Peraturan Anggota Dewan Gubernur Nomor 24 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia.

Bank Indonesia. (2024c). Peraturan Bank Indonesia Nomor 3 Tahun 2024 tentang Lembaga Alternatif Penyelesaian Sengketa di Sektor Keuangan.

Bank Indonesia. (2025a). Laporan Perekonomian Indonesia 2024.

Bank Indonesia. (2025b). Laporan Kelembagaan Bank Indonesia 2024.

Bank Indonesia. (2025c). Laporan Kebijakan Moneter Triwulan IV 2024.

Bank Indonesia. (2026). Peraturan Bank Indonesia Nomor 6 Tahun 2026 tentang Pelindungan Konsumen Bank Indonesia.

Committee on Payments and Market Infrastructures, & International Organization of Securities Commissions. (2016). Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements.

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. ACM Computing Surveys, 54(8), Article 173, 1–35. https://doi.org/10.1145/3469886

Financial Services Authority. (2023). Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.

Financial System Stability Committee. (2026). Kondisi sistem keuangan tetap resilien, didukung koordinasi dan sinergi kebijakan antarotoritas dengan tetap mewaspadai dinamika dan risiko global [Joint press release].

Hadjon, P. M. (1987). Perlindungan hukum bagi rakyat di Indonesia. Bina Ilmu.

Koskelainen, T., Kalmi, P., Scornavacca, E., & Vartiainen, T. (2023). Financial literacy in the digital age—A research agenda. Journal of Consumer Affairs, 57(1), 507–528. https://doi.org/10.1111/joca.12510

Muhammad, A. K. (2004). Hukum dan penelitian hukum. Citra Aditya Bakti.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against phishing attacks: A systematic literature review. Computers & Security, 132, Article 103387. https://doi.org/10.1016/j.cose.2023.103387

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

OECD. (2022). G20/OECD high-level principles on financial consumer protection 2022. OECD Publishing. https://doi.org/10.1787/48cc3df0-en

Panos, G. A., & Wilson, J. O. S. (2020). Financial literacy and responsible finance in the FinTech era: Capabilities and challenges. The European Journal of Finance, 26(4–5), 297–301. https://doi.org/10.1080/1351847X.2020.1717569

Pratiwi, R., Prabowo, M. S., Nugroho, M., & Wardhani, W. N. R. (2022). Fraud risk in peer lending fintech transactions: The role of consumer protection regulation in Indonesia. International Journal of Social Science and Business, 6(4), 469–477. https://doi.org/10.23887/ijssb.v6i4.46511

Republic of Indonesia. (1999). Law Number 8 of 1999 concerning Consumer Protection.

Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection.

Republic of Indonesia. (2023). Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector.

Republic of Indonesia. (2024). Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Sarno, D. M., & Black, J. (2024). Who gets caught in the web of lies? Understanding susceptibility to phishing emails, fake news headlines, and scam text messages. Human Factors, 66(6), 1742–1753. https://doi.org/10.1177/00187208231173263

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review, 57, Article 324. https://doi.org/10.1007/s10462-024-10973-2

Soekanto, S. (2018). Faktor-faktor yang memengaruhi penegakan hukum. Rajawali Pers.

Soekanto, S., & Mamudji, S. (2019). Penelitian hukum normatif: Suatu tinjauan singkat. Rajawali Pers.

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D. M., & Russello, G. (2023). SoK: Human-centered phishing susceptibility. ACM Transactions on Privacy and Security, 26(3), Article 21, 1–27. https://doi.org/10.1145/3575797