Legal Protection for Banking Customers Against Personal Data Breaches in Open Banking Services in Indonesia

Aliyah Pratiwi Hatta[1], Subekti[2], Muhamad Yustina Ariwibawa [3], Vallencia Nandya Paramitha [4]

[1-4]Faculty of Law, Universitas Dr. Soetomo, Indonesia
✉ Corresponding email: aliyahpratiwihatta@gmail.com

History of Article
Submitted : April 20, 2026
Revised : April 28, 2026
Accepted : May 26, 2026
Published : June 01, 2026
DOI : https://doi.org/10.37253/jjr.v28i1.12312

Copyright© 2026 by Author(s). This work is licensed under a Creative Commons Attribution-Non Commercial-Share Alike 4.0 International License. All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions.

Abstract

The expansion of open banking services improves digital financial connectivity while increasing the risk of personal data breaches across banks, payment service providers, and collaborating entities. This study analyzes the legal protection available to banking customers in Indonesia and formulates an accountability model for incidents involving multiple actors. It employs normative legal research with doctrinal, statutory, conceptual, and analytical approaches. Primary and secondary legal materials were collected through document study and examined qualitatively through legal interpretation, norm synchronization, and prescriptive analysis. The findings show that Indonesia has established preventive safeguards through personal data protection law, financial consumer protection rules, electronic system governance, cybersecurity standards, and the National Standard for Open Application Programming Interface Payments. However, responsibilities remain distributed across regulatory regimes, creating uncertainty after a breach. This study proposes an integrated accountability and redress model based on functional role classification, limited data access, partner supervision, coordinated notification, a single-entry complaint mechanism, evidence preservation, and proportionate remediation. The study recommends a coordinated protocol involving Bank Indonesia, the Financial Services Authority, and the personal data protection supervisory institution. Future research should evaluate its implementation within banking institutions and digital payment ecosystems. It also identifies priorities for cross-border processing and customer-facing consent management.

Keywords: Open Banking; Personal Data Breach; Banking Customers.

Introduction

The expansion of digital financial services has transformed personal data into a central asset of banking transactions. In open banking services, banks no longer operate as closed institutions that retain customer information within an internal system, because data may be exchanged through application programming interfaces with payment service providers, financial technology companies, and other collaborating entities (Karthika M. et al., 2022; Librawenson, Disemadi & Afdal, 2025). This model offers efficiency, interoperability, and broader access to financial products, but it also increases the points at which personal data may be exposed, misused, or unlawfully disclosed (Ghosh et al., 2023). This technological expansion shifts the legal problem from mere system connectivity to the question of who bears responsibility when personal financial data are breached across multiple entities (Nurlaily et al., 2025; Agustianto et al., 2026). The legal issue is therefore not limited to technological security, because it concerns the extent to which customers remain protected when their financial information circulates across an interconnected service ecosystem.

The urgency of this issue becomes clearer when a personal data breach is viewed from the position of a banking customer (Diyanatalia, Sudirman & Disemadi, 2025). A customer may consent to a digital service without fully understanding which entities will receive the data, how long it will be retained, or which party must respond when an incident occurs. A breach may originate from the bank, a payment service provider, a nonbank partner, an outsourced processor, or a weakness in the interface connecting those actors (Javaheri et al., 2024; Amboro, Macnico, Tan & Bajury, 2025). In such circumstances, the customer faces difficulty in identifying the responsible party and obtaining a remedy for financial loss, privacy violation, and further misuse. In this setting, the core legal problem is not only the occurrence of the breach, but the uncertainty of responsibility allocation, complaint handling, and effective customer redress.

Financial data requires a high level of protection because its disclosure may reveal transaction patterns, economic capacity, account relationships, and information capable of affecting an individual's security (van Zeeland & Pierson, 2024). Law Number 27 of 2022 on Personal Data Protection places financial data within the category of specific personal data, while recognizing the rights of data subjects and the obligations of controllers and processors throughout the processing cycle (Saputra, 2024). The significance of this framework is reinforced by the reality that personal data violations are not hypothetical in Indonesia's digital environment (Bella Fistya Asherli & Sidi Ahyar Wiraguna, 2025). A Bank Indonesia research paper reported that the Ministry of Communication and Informatics identified ninety eight alleged personal data protection violations from 2019 to 2023, including data leakage.

Indonesia has responded to digital payment integration through the National Standard for Open Application Programming Interface Payments, commonly known as SNAP. The framework is implemented through Bank Indonesia Regulation Number 23/11/PBI/2021 on the National Standard for Payment Systems and Regulation of the Members of the Board of Governors Number 23/15/PADG/2021 on the National Standard for Open Application Programming Interface Payments (Sarif & Ariyanti, 2024). SNAP defines an open payment API as an interface whose connectivity is granted under a cooperation agreement between service providers and service users for payment transaction processing. It covers interoperability, information system security, governance, and risk management, confirming that data exchange cannot be separated from institutional accountability.

The legal structure surrounding open banking developed further after the enactment of the Personal Data Protection Law. Bank Indonesia Regulation Number 3 of 2023 strengthened the consumer protection framework within the scope of Bank Indonesia's authority, while Financial Services Authority Regulation Number 22 of 2023 established a broader framework for consumer and public protection in the financial services sector. Bank Indonesia Regulation Number 2 of 2024 subsequently addressed information system security and cyber resilience for payment system providers and other parties regulated and

supervised by Bank Indonesia. These instruments indicate a progressive response, but they also create a multilayered framework that must be interpreted coherently when a customer seeks protection after an incident.

Although these regulations establish preventive duties, they do not yet provide a sufficiently clear post-breach framework for banking customers. The main weakness lies not in the absence of norms, but in the fragmentation of supervisory authority, the overlap of legal categories across banking, payment systems, and personal data protection law, and the lack of a clear customer-facing mechanism for identifying the responsible actor, filing a complaint, and obtaining compensation after a breach.

The principal difficulty lies in the relationship between sectoral supervision and the personal data protection regime. Open banking activities may involve banks supervised by the Financial Services Authority, payment system providers regulated by Bank Indonesia, electronic system operators, and third parties that receive or process customer data under a cooperation agreement(Adedoyin Tolulope Oyewole et al., 2024). The Personal Data Protection Law also mandates an institution responsible for administering personal data protection, including policy formulation, supervision, administrative enforcement, and dispute resolution outside the courts (Purwanti et al., 2025). During institutional transition, the division of supervisory responsibility may create uncertainty regarding coordination, enforcement sequence, and the forum most accessible to an affected customer.

A personal data breach in open banking cannot be treated merely as a failure to preserve secrecy. Traditional banking law was designed around a relationship in which the bank controlled customer information within an identifiable institutional boundary, whereas open banking introduces distributed data control and processing (Zeynalova, 2024). The legal analysis must therefore distinguish bank secrecy, personal data protection, consumer protection, electronic system security, and cyber resilience without isolating those fields from one another. This distinction is necessary because legal consequences may differ according to the breached data, each actor's role, the source of failure, and the harm suffered by the customer.

The question of consent also requires careful examination in contemporary practice. In open banking, consent is often presented through digital interfaces and may function as the legal basis for access to customer information. However, consent cannot be reduced to a procedural click when the customer lacks meaningful information about the purpose of processing, the recipients of the data, the retention period, and the consequences of withdrawal (Naudts et al., 2022). A legally valid consent mechanism must be connected to transparency, purpose limitation, proportionality, security safeguards, and a clear method for terminating access when the customer no longer wishes to share data.

Existing studies have provided an important foundation for understanding these developments. Billiam, Abubakar, and Handayani (2022) examined the urgency of open API standardization and concluded that data sharing between banks and financial technology companies or electronic commerce platforms had previously depended heavily on agreements between the parties. Their study showed that differences in API standards could affect customer data protection and that SNAP offered a more structured basis for connectivity (Sakti et al., 2024). This contribution remains relevant, but it emerged during an earlier regulatory phase and therefore did not fully address the implications of the Personal Data Protection Law, the strengthened consumer protection framework, or the later cyber resilience regulation.

Amalia et al. (2022) also examined personal data protection and consumer protection in open API payments through a normative juridical approach (Amalia, 2022). Their study found that the rules existing at that time addressed several legal aspects while leaving a need for stronger statutory protection. The enactment of Law Number 27 of 2022 and Financial Services Authority Regulation Number 22 of 2023 changed the relevant legal context. The question is now whether the combined general and sectoral rules provide effective remedies after an actual breach.

Comparative scholarship has further demonstrated that the quality of open banking governance depends on institutional design. Fajri (2024) compared Indonesia and the United Kingdom and highlighted the importance of a more specific implementation and supervisory structure for strengthening legal

certainty and public trust. Pati et al. (2025) similarly argued that an effective regulatory approach must be designed according to the particular objectives pursued by a country in adopting open banking (Pati & Pratama, 2025). These studies broaden the policy discussion, but a comparative or design oriented approach still needs to be complemented by a closer analysis of responsibility allocation and customer remedies in the Indonesian regulatory setting.

Despite these contributions, the current literature still leaves a specific gap. Many studies focus on the desirability of standardization, the adequacy of general data protection norms, comparative institutional models, or the broader regulatory direction of open banking. Fewer studies place the personal data breach itself at the center of the legal analysis and trace the customer's position from the moment of unauthorized disclosure through notification, complaint handling, attribution of responsibility, dispute resolution, and compensation. This omission is important because a regulatory framework should not be assessed only by the existence of preventive obligations, but also by its capacity to provide a predictable response after protection has failed.

A further issue concerns the relationship between technical compliance and substantive legal protection. Compliance with API standards, information security procedures, verification requirements, and cyber resilience policies is essential, but it does not eliminate the possibility of an incident. When a breach occurs, the customer needs timely notification, an accessible complaint mechanism, preservation of evidence, corrective measures, and a legally intelligible route to compensation (Masuch et al., 2021). The effectiveness of legal protection must therefore be measured through both preventive safeguards and repressive remedies, rather than through formal compliance with technical standards alone.

Based on this background, this study addresses two questions: how Indonesian law regulates the protection of banking customers against personal data breaches in open banking services, and what accountability model is needed when breaches involve multiple actors. This study aims to assess the coherence of the applicable regulatory framework and to formulate a customer-centered post-breach protection model. Its original contribution lies in shifting the analysis

from general regulatory adequacy to a breach-centered examination of notification, complaint handling, responsibility allocation, and redress in Indonesia's digital financial ecosystem.

Research Method

This study employs normative legal research with a doctrinal design, supported by statutory, conceptual, and analytical approaches, because the research questions concern the coherence of legal norms and allocation of responsibility in personal data breaches within open banking services. The object of analysis consists of primary legal materials relating to personal data protection, banking, consumer protection, electronic systems, payment systems, and the National Standard for Open Application Programming Interface Payments. The primary legal materials specifically analyzed include Law Number 27 of 2022 on Personal Data Protection, Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998, Law Number 8 of 1999 on Consumer Protection, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions, Bank Indonesia Regulation Number 23/11/PBI/2021 on the National Standard for Payment Systems, Regulation of the Members of the Board of Governors Number 23/15/PADG/2021 on the National Standard for Open Application Programming Interface Payments, Bank Indonesia Regulation Number 3 of 2023 on Consumer Protection within the Scope of Bank Indonesia, Financial Services Authority Regulation Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector, Bank Indonesia Regulation Number 2 of 2024 on Information System Security and Cyber Resilience, and the relevant SNAP Governance Guidelines. Secondary legal materials comprise scholarly articles, books, research reports, and institutional publications discussing open banking, data governance, cybersecurity, and customer protection. The materials were selected purposively based on normative relevance, regulatory authority, recency, and connection to customer rights, data processing obligations, breach management, and legal remedies. In addition, the documentary data examined in this study include official policy and governance documents relevant to consent

management, access validation, partner supervision, breach notification, complaint handling, and compensation routes in open banking services.

Data were collected through a document study conducted in four stages: identification of applicable regulations, classification of legal materials, examination of scholarly interpretations, and comparison of provisions governing preventive protection and post-breach remedies. The research instrument was a document review matrix containing categories of legal basis, regulated actor, type of obligation, form of liability, supervisory authority, complaint mechanism, sanction, and compensation route. The collected materials were analyzed qualitatively through legal interpretation, norm synchronization, and prescriptive analysis by mapping horizontal and vertical consistency, identifying regulatory gaps, and assessing whether the framework provides effective customer protection. The analysis concludes with the formulation of an integrated accountability model for open banking services that connects consent, security, breach notification, supervision, dispute resolution, and compensation.

Results and Discussions

The Normative Architecture of Banking Customer Protection Against Personal Data Breaches in Open Banking Services

The normative analysis demonstrates that open banking in Indonesia must be understood within a specific regulatory context. Indonesia has not established a single legislative regime that comprehensively regulates banking data portability, third-party access, and personal financial management services under a unified open banking statute. The most concrete operational framework is the National Standard for Open Application Programming Interface Payments, commonly referred to as SNAP, which regulates the interconnection of payment services through standardized interfaces (Billiam et al., 2022). Accordingly, the term open banking in this study refers to banking-related data access and payment connectivity conducted through an interconnected digital ecosystem,

particularly Open API Payments involving banks, payment service providers, and collaborating entities.

This conceptual qualification is necessary because the legal protection of customers depends on the actual scope of the regulated activity. An Open API Payments arrangement may involve access to customer profiles, transaction instructions, account-related information, authentication data, and underlying payment data, although the precise data set depends on the service used (Wolters & Jacobs, 2019). The banking customer is therefore positioned within a chain of processing activities that may extend beyond the bank's internal information system. The risk is no longer confined to an unauthorized disclosure by a bank employee, because exposure may occur during transmission, authentication, storage, application integration, third-party processing, or incident response.

The doctrinal review identified a multilayered regulatory framework governing the protection of banking customers. The first layer consists of Law Number 27 of 2022 on Personal Data Protection, which provides general principles, data subject rights, controller obligations, processor obligations, breach notification requirements, sanctions, and dispute resolution mechanisms. The second layer includes banking regulation, consumer protection rules, payment system regulation, electronic system governance, technology information governance for commercial banks, and cybersecurity resilience standards. The third layer consists of contractual and technical standards governing cooperation among service providers, payment service provider users, and non-payment service provider users within the SNAP ecosystem.

The relationship among these layers is complementary, but it is not entirely seamless. The Personal Data Protection Law uses the language of data subjects, personal data controllers, and personal data processors (Situmeang, Disemadi & 2024), while financial sector regulations use the language of consumers, financial services businesses, service providers, service users, payment service providers, and non-payment service provider users (Taufiq, 2025). These categories may overlap in practice, but they do not always produce an immediately visible allocation of responsibility for an affected customer. A central finding of this study is therefore that Indonesia possesses a substantial body of preventive

regulation, yet its application after a breach requires a clearer interpretative framework.

This lack of seamlessness has direct legal consequences for customers after a breach. Conceptual overlap between controller-processor categories under personal data protection law and actor categories under sectoral financial regulation may obscure who must notify the customer, who must preserve evidence, and which institution bears the first obligation to provide remedial assistance. As a result, a framework that is normatively dense may still operate as practically uncertain from the customer's perspective when a breach moves across institutional and contractual boundaries.

TABLE 1. Normative Architecture of Banking Customer Protection in Open Banking Services in Indonesia

No	Normative Layer	Primary Regulatory Basis	Main Protection Mechanism	Principal Interpretative Issue
1	General personal data protection.	Law Number 27 of 2022.	Lawful processing, data subject rights, security, breach notification, sanctions, and compensation.	Classify each actor by its actual processing role.
2	Banking and consumer protection.	Banking Law and POJK Number 22 of 2023.	Confidentiality, informed consent, partner safeguards, transparency, and complaint handling.	External partners cannot dilute sectoral duties.
3	Electronic systems and cyber resilience.	Government Regulation Number 71 of 2019 and PBI Number 2 of 2024.	Reliable systems, confidentiality, integrity, availability, response, recovery,	Coordinate cyber reporting and personal data

			and cyber resilience.	breach notification.
4	Open API Payments governance.	PADG Number 23/15/PADG/2021 and SNAP Governance Guidelines.	Interoperability, authentication, access validation, testing, consent, partner supervision, and revocation.	Connect standardized interfaces with enforceable remedies.
5	Processed finding.	Author's normative synthesis	Substantial preventive safeguards exist across several regulatory regimes.	Integrate responsibility, evidence, complaints, remedies, and regulatory coordination.

Source: Processed by the author based on the applicable Indonesian regulations.

The processed normative findings are summarized in Table 1. The table identifies the principal legal instruments, their regulatory focus, the actors primarily addressed, the protective mechanisms, and the remaining issues requiring legal interpretation. It does not reproduce every statutory provision, because the purpose of the table is to reveal the relationship among the rules rather than to restate raw legislative text. The table serves as the foundation for evaluating whether the present framework produces effective legal protection for banking customers.

To operationalize Table 1, the present study proposes a sequential interpretative approach for breach cases. The first step is to identify the actor that directly determined the purpose and means of the relevant data processing, because this classification is necessary for assigning primary duties under personal data protection law. The second step is to identify whether a regulated bank, payment service provider, or other supervised entity remained under a sectoral duty to protect customer data despite outsourcing or cooperation. The third step is to determine whether the incident also involved electronic system failure, cyber

resilience obligations, or SNAP governance duties relating to access validation, consent, testing, and partner supervision. The fourth step is to assess which institution must provide the first customer-facing response, including notification, complaint registration, and evidence preservation, even before final attribution is completed. Through these steps, Table 1 functions not only as a descriptive synthesis, but as a doctrinal guide for regulators, courts, and complaint-handling bodies when assessing responsibility in a specific breach.

Table 1 reveals that personal financial data protection in open banking services cannot be derived from bank secrecy alone. Article 4 of the Personal Data Protection Law classifies personal financial data as specific personal data, reflecting the sensitivity of information that may expose a person's economic condition and transaction behavior. This classification is legally significant because the level of protection must be calibrated according to the nature and risk of the processed data. The transmission of banking data through interoperable services therefore requires a level of diligence proportionate to the possibility of fraud, profiling, identity misuse, unauthorized transactions, and further dissemination.

The lawful processing of personal data must be distinguished from the mere technical possibility of accessing the data. Article 20 of the Personal Data Protection Law requires a lawful basis for processing, which may include explicit valid consent, contractual necessity, legal obligation, vital interests, public duties, or other legitimate interests subject to statutory conditions (Alkhamsi & Alqahtani, 2024). In open banking services, consent frequently becomes the most visible legal basis because customers authorize access through digital interfaces. However, the existence of a digital confirmation does not automatically establish that every subsequent use, retention, transfer, or disclosure remains lawful.

Consent must be evaluated in relation to purpose, scope, duration, recipients, and the possibility of withdrawal. A customer who authorizes a payment initiation service does not necessarily authorize the recipient to use transaction data for unrelated profiling, commercial targeting, or redistribution to another entity. The principle of purpose limitation prevents an authorization

from becoming an unlimited license for data exploitation (Nuredini et al., 2022). This distinction is essential because open banking innovation should not be developed through broad-form consent language that deprives customers of effective control over personal financial information.

Articles 35 to 39 of the Personal Data Protection Law establish a coherent security obligation. Controllers must adopt technical and operational measures, determine the required level of security according to the nature and risk of the data, maintain confidentiality, supervise parties involved in processing under their control, prevent unlawful processing, and prevent unauthorized access (Syailendra, 2024; Guari, Situmeang & Disemadi, 2026). These obligations are particularly relevant when a bank or payment service provider engages another entity to support a digital service. The use of an external processor does not eliminate the controller's duty to supervise processing activities conducted within the operational chain.

The obligation to record processing activities also has a central evidentiary function. Article 31 requires personal data controllers to record all personal data processing activities, while Article 32 gives data subjects access to processed personal data and its processing record subject to statutory conditions. In open banking, a reliable audit trail is needed to determine which entity accessed the data, at what time, for what stated purpose, through which interface, and under which authorization (Zachariadis & Ozcan, 2016). Without an intelligible record, the formal recognition of customer rights becomes difficult to enforce in practice.

The Personal Data Protection Law also regulates breach notification. Article 46 requires the controller to provide written notification no later than three times twenty-four hours after a personal data protection failure occurs, addressed to the data subject and the relevant institution (Sari, 2023). The notification must at least identify the disclosed data, explain when and how the disclosure occurred, and describe the handling and recovery measures undertaken by the controller. This requirement places the customer in a position to take protective action, but its effectiveness depends on whether the responsible controller can be identified promptly within a multi-actor ecosystem.

Personal data protection and bank secrecy should not be treated as interchangeable concepts (Diyanatalia, Sudirman & Disemadi, 2025). Bank secrecy focuses on a defined category of banking information and a duty of confidentiality imposed on banks, while personal data protection governs the entire processing cycle and applies to controllers and processors according to their actual activities (Rannie B., 2023). A data set may require protection under the Personal Data Protection Law even when it falls outside a narrow interpretation of depositor information and deposits. Conversely, a bank may remain subject to confidentiality duties even when another lawful basis permits a limited form of personal data processing for a specified purpose.

POJK Number 22 of 2023 reinforces this conclusion within the financial services sector. Article 19 requires financial services businesses to maintain the confidentiality and security of consumer data and information, including other data provided or made accessible by consumers. When a financial services business cooperates with another party to manage customer data or information, it must ensure that the cooperating party maintains confidentiality and security (Florence Olweny, 2024). This provision is important because it prevents a regulated financial institution from treating a cooperation agreement as a complete transfer of regulatory responsibility.

The bank's duty of prudence does not end when an external service provider is involved. Outsourcing or collaboration may redistribute technical tasks, but the bank remains required to evaluate the service provider, define obligations, monitor performance, secure information, prepare continuity measures, and respond to risk events (Anderson-Princen, 2022). This principle is consistent with the accountability approach under the Personal Data Protection Law. A regulated bank should not be able to rely on organizational complexity as a defense against a customer's claim that the service architecture failed to provide adequate protection.

The SNAP framework adds specific rules for Open API Payments. Bank Indonesia established SNAP to support a healthy, competitive, innovative, integrated, interconnected, interoperable, secure, and reliable payment system industry. PADG Number 23/15/PADG/2021 governs the implementation of

Open API Payments based on SNAP and requires service providers and payment service provider users to apply the relevant technical, security, data, and governance standards (Amalia, 2022). This regulatory design reflects the understanding that interoperability must be accompanied by standardized control mechanisms.

PADG Number 23/15/PADG/2021 requires service providers and payment service provider users to conduct a consumer consent process before accessing customer data in transaction processing (Amalia, 2022). The process includes verification or authentication of the identity of the party accessing the data and validation of that party's access rights. Consent may be required for each access or may apply for a specified period until revoked, depending on the type of Open API Payments service and the original purpose. A service provider must stop transaction processing or data access when the required authorization or consent process fails.

The SNAP framework also imposes obligations relating to system development and testing. Service providers and payment service provider users must conduct tests through the SNAP Developer Site, perform functionality testing, maintain documentation for system development, changes, and maintenance, request verification from the relevant self-regulatory organization, and comply with applicable laws. Functionality testing must cover connected systems and relevant scenarios, including positive and negative scenarios. These obligations reduce the possibility that an interface will be deployed without assessing foreseeable failures and security vulnerabilities.

The regulation pays particular attention to non-payment service provider users. A service provider working with a Non-PJP Service User must ensure that the cooperating entity applies SNAP, complies with applicable obligations, implements the consumer consent mechanism, and satisfies relevant development and testing requirements. The service provider must also ensure that the Open API Payments contract conforms to the contractual standards in the governance guidelines. This approach recognizes that an unregulated or differently regulated entity may introduce risks into an otherwise supervised payment ecosystem.

Cyber resilience regulation provides an additional level of protection. PBI Number 2 of 2024 and PADG Number 24 of 2024 require relevant providers regulated and supervised by Bank Indonesia to maintain information system security and cybersecurity resilience. The framework is built around confidentiality, integrity, availability, business continuity, anticipatory action, adaptive measures, proactive controls, incident response, and rapid recovery (Amirulloh et al., 2025). This structure is aligned with the broader concept of a personal data protection failure under the Personal Data Protection Law.

The normative analysis identifies at least five forms of fragmentation. The first is conceptual fragmentation between bank secrecy, personal data protection, consumer protection, and cybersecurity resilience. The second is institutional fragmentation involving OJK, Bank Indonesia, the personal data protection supervisory institution, electronic system governance authorities, and dispute resolution bodies. The third is relational fragmentation because the service may involve a bank, a payment service provider, a non-payment service provider user, an outsourced processor, and a technology vendor.

Each form of fragmentation produces a different legal difficulty. Conceptual fragmentation makes it harder to classify duties of confidentiality, data processing, and post-breach notification within one intelligible legal sequence. Institutional fragmentation creates uncertainty over which regulator, complaint forum, or supervisory body should be approached first by an affected customer. Relational fragmentation complicates the attribution of fault because several actors may participate in the same processing chain without being equally visible to the customer. In practice, these forms of fragmentation may delay complaint handling, weaken evidentiary access, and shift the burden of legal reconstruction onto the customer, even though the relevant information is controlled by institutions within the service ecosystem.

Fragmentation affects the customer's bargaining position. Banks and collaborating entities possess technical information, contractual documentation, internal audit records, incident reports, and access logs that are not ordinarily available to customers. A customer may know that suspicious activity or unauthorized disclosure occurred but may not know where the failure

originated. The imbalance of information makes it unreasonable to place the initial burden of reconstructing the entire processing chain on the affected customer.

A stylized example may clarify this difficulty. A bank grants account-related access to a PJP through Open API Payments, and the PJP in turn cooperates with a Non-PJP Service User that uses transaction data for an auxiliary digital service. If customer data are later disclosed or reused beyond the authorized purpose, the customer may not know whether the breach originated from the bank's access controls, the PJP's retention practices, or the Non-PJP Service User's downstream processing. At the same time, the legal categories applied to those actors may differ across the Personal Data Protection Law, payment system regulation, and contractual governance. This overlap hinders the customer's ability to identify the proper defendant, choose the initial complaint route, and obtain timely redress.

The principal result of the first sub-discussion is that legal protection exists but remains normatively distributed. A distributed framework is capable of providing effective protection only when roles, procedures, and remedies are connected through an intelligible accountability structure. The bank remains a central actor because it holds the customer relationship, administers sensitive financial data, and possesses the capacity to evaluate cooperating entities. The second sub-discussion therefore examines how an integrated responsibility and redress model should operate when preventive protection fails.

This normative synthesis also clarifies the article's distinction from earlier Indonesian open banking scholarship. Previous studies were important in emphasizing API standardization, statutory protection, and regulatory design, but they generally did not translate regulatory overlap into an accountability structure that can be used after a personal data breach. The present analysis moves further by showing that the central weakness of the Indonesian framework lies not merely in incomplete regulation, but in the absence of an operational interpretative structure linking actor classification, supervisory duties, evidence, complaints, and remedies within a multi-actor breach.

An Integrated Accountability and Redress Model for Personal Data Breaches in Open Banking Services

The analysis of post-breach protection begins with a distinction between preventive protection and corrective protection. Preventive protection consists of lawful processing, informed consent, secure architecture, testing, monitoring, documentation, risk assessment, cybersecurity resilience, and supervision of collaborating parties. Corrective protection begins when confidentiality, integrity, or availability has failed and the customer requires notification, assistance, investigation, restoration, compensation, and a clear dispute resolution route. A legally adequate framework must contain both dimensions because innovation cannot be evaluated only from the existence of rules designed to prevent incidents.

A breach-centered approach changes the focus of legal analysis. Instead of asking only whether an institution has adopted policies, the analysis asks what happens to a customer after a specific failure occurs. It examines which institution must receive the complaint, which actor must provide the first response, which logs must be preserved, which notification must be issued, which regulator must be informed, and how compensation must be assessed. This approach is necessary because the practical quality of legal protection becomes visible when an incident tests the architecture of responsibility.

In practical terms, the proposed model operates through four immediate post-breach functions: first response, complaint access, evidence control, and remediation. This structure is important because a customer-facing model should not merely identify abstract duties, but should clarify who responds first, where the complaint enters, how relevant records are preserved, and how interim and final remedies are delivered.

An open banking breach may originate from several points in the processing chain. The bank's system may fail to validate an access token, a payment service provider may retain data beyond the authorized period, a Non-PJP Service User may process information for an unrelated purpose, an outsourced technology vendor may expose credentials, or an interface may transmit information through an insecure configuration (Modesti et al., 2025). A breach may also

result from a combination of errors rather than a single identifiable action. The legal framework must therefore accommodate distributed causation without allowing the customer to become trapped in a dispute among institutions.

The concept of personal data controller is central to the allocation of responsibility. A controller determines the purposes of processing and exercises control over the processing of personal data, while a processor processes personal data on behalf of a controller. In practice, an open banking arrangement may involve one controller, several controllers exercising distinct purposes, joint controllers determining aspects of processing together, or processors operating under documented instructions. The legal classification must be based on actual conduct rather than the terminology selected in a commercial contract.

A bank may act as a controller when it determines the purposes and means of processing customer data for banking and payment services. A payment service provider may also act as a controller when it independently determines how data are used for a service it offers to the customer. A technology vendor may function as a processor when it stores or transmits data solely under documented instructions without deciding the commercial purpose (Dahi & Compagnucci, 2022). A Non-PJP Service User may become an independent controller if it uses data for its own profiling, marketing, product design, or other purposes beyond a narrowly instructed processing task.

The bank nevertheless occupies a distinct position in the ecosystem. It administers the customer relationship, holds sensitive financial data, provides access to the source of funds, and is subject to banking prudence, financial consumer protection, technology governance, and personal data obligations. The bank is also ordinarily better positioned than the customer to evaluate whether a proposed partner satisfies legal and technical requirements (Karwati et al., 2024). These features justify treating the bank as a primary point of accountability for customer-facing response, even when another actor ultimately caused the incident.

A concise scenario illustrates this allocation. A customer authorizes a bank account connection for a payment initiation service operated by a PJP, and the PJP cooperates with a Non-PJP Service User that stores transaction-related data

for an auxiliary commercial feature. If the data are later disclosed beyond the authorized purpose, the customer will ordinarily know the bank and the visible service interface, but not the internal contractual and technical chain behind the breach. In this situation, requiring the customer to identify the ultimate wrongdoer before receiving assistance would undermine effective protection. For that reason, the bank or the institution directly interfacing with the customer should bear the first customer-facing duty, while final liability may later be allocated according to actual control, fault, and contribution.

Primary customer-facing accountability does not necessarily mean that the bank must bear every final financial consequence. The model proposed in this study separates immediate customer protection from internal allocation of liability among business actors. The customer should be able to report an incident through the bank or the provider with which the customer directly interacts and receive coordinated assistance without first proving which institution caused the breach (Thomas & Sule, 2023). After the customer's urgent interests have been protected, the participating institutions may pursue contractual recourse or contribution according to their respective failures. This distinction prevents two doctrinal errors at once, namely treating the bank as the sole substantive wrongdoer in every case, and denying the customer immediate assistance until the internal allocation of fault has been completed.

The proposed accountability model consists of several levels. The first level is direct responsibility, which applies to the institution that determines the purpose of processing, controls the relevant system, or commits the unlawful act. The second level is supervisory responsibility, which applies when a bank or service provider fails to evaluate, monitor, or control a collaborating party as required by law and the SNAP framework. The third level is coordinated remedial responsibility, which requires customer-facing institutions to provide assistance even when final attribution remains under investigation (Thomas & Sule, 2023).

The use of multiple levels avoids two opposite errors. The first error is to impose responsibility exclusively on the bank without examining the independent unlawful conduct of other actors. The second error is to allow every

institution to refer the customer elsewhere until technical causation has been conclusively established. An integrated model preserves the possibility of differentiated final liability while ensuring that customers receive an accessible and timely remedy.

Breach notification is the first component of corrective protection. Article 46 of the Personal Data Protection Law requires a written notification no later than three times twenty-four hours after the occurrence of a personal data protection failure. The notification must identify the disclosed data, explain when and how exposure occurred, and describe the measures taken to manage and recover from the incident (Algamar et al., 2024). For open banking services, the notification should also explain the relevant service, the affected access permission, the cooperating entities involved, and the practical steps available to the customer.

The complaint mechanism is the second component of corrective protection. A banking customer should not be required to select the legally correct regulator or business entity at the beginning of the process. The institution receiving the complaint should register the matter, issue a receipt, apply immediate protective measures, and coordinate with other relevant entities. A single-entry complaint principle would reduce the procedural burden created by fragmented institutional roles.

The single entry principle should therefore be understood as a rule of access rather than a rule of final competence. Its immediate function is to prevent complaint rejection at the entry point. Once a complaint is received, the receiving institution should be under a duty to register the matter, trigger basic protective measures, preserve or request preservation of available evidence, and forward the case through documented channels without interrupting communication with the customer.

The single entry principle does not eliminate the jurisdiction of each authority. It operates as an access mechanism that ensures a complaint is not rejected merely because another participant may have caused the failure. The receiving institution should transmit relevant information to cooperating entities and regulators according to documented procedures. The customer should

receive a consolidated explanation of the handling process and the institution responsible for communicating progress.

Evidence preservation is the third component of the model. Personal data breaches in open banking services are often difficult to prove because relevant evidence is digital, distributed, and controlled by the institutions involved. Access logs, consent records, authentication results, token histories, system alerts, transaction records, testing documentation, vendor reports, internal communications, and forensic findings may become decisive (Algamar et al., 2024). The law should therefore require preservation of relevant evidence from the moment an incident is detected or reasonably suspected.

This conclusion supports an accountability-based evidentiary approach. The customer should establish an initial credible indication of harm, unauthorized access, suspicious activity, or a relevant breach notification. Once that threshold is met, the institutions controlling the evidence should explain the processing chain and demonstrate compliance with security, consent, monitoring, and incident handling obligations. This is not an automatic presumption that every incident proves negligence, but it recognizes the imbalance of information between customers and digital financial service providers.

Compensation is the fourth component of corrective protection. Article 12 of the Personal Data Protection Law recognizes the data subject's right to file a claim and receive compensation for violations concerning the processing of personal data. Consumer protection rules also provide a basis for seeking remedies when a service causes loss (Sudirman et al., 2023). The challenge is to develop a compensation approach that recognizes the range of harms arising from personal financial data breaches.

The most visible form of harm is direct financial loss. Unauthorized transactions, fraudulent credit applications, account takeover, identity misuse, recovery expenses, and the costs of replacing credentials may be documented through financial records. These losses should be assessed promptly, particularly when delayed restoration increases the customer's exposure (Romanosky, 2016).

An effective remedy should not force the customer to wait for the final allocation of liability among institutions before receiving urgent assistance.

In breach cases involving payment access, compensation should also be viewed in temporal stages. Urgent interim relief may include transaction blocking, credential replacement, temporary reimbursement for clearly documented loss, and restoration of account security, while final compensation may depend on fuller attribution and assessment of responsibility. This staged approach is necessary because customer protection may fail in practice if immediate restoration is postponed until all institutional disputes have been settled.

Non-material harm requires careful legal consideration. The disclosure of personal financial data may interfere with privacy, create anxiety, expose a person's economic behavior, and undermine trust in digital financial services. Not every inconvenience should automatically produce an excessive claim, but the absence of a completed fraudulent transaction does not mean that the breach is legally insignificant. Courts and dispute resolution bodies need a reasoned approach for assessing the seriousness, duration, scope, sensitivity, and foreseeable consequences of the exposure. A breach-centered model should therefore require adjudicators and complaint-handling bodies to evaluate non-material harm not only by the existence of completed fraud, but also by the seriousness of exposure, loss of control over sensitive financial data, duration of uncertainty, and the reasonable foreseeability of further misuse.

Compensation should be distinguished from administrative sanctions. Administrative sanctions serve regulatory objectives, including deterrence, compliance, market discipline, and correction of institutional behavior. Compensation serves the restoration of the affected person's rights and losses. An administrative fine imposed on an institution does not automatically repair the harm suffered by a customer (Li, 2023).

The Personal Data Protection Law provides administrative and judicial mechanisms, while financial sector regulations provide complaint handling, supervisory action, and sanctions within their respective scopes. These routes should operate in a complementary manner. A customer may pursue a complaint

through the relevant provider, use the available financial sector dispute resolution mechanism, submit information to the appropriate regulator, or pursue a civil claim according to applicable law. The existence of several routes should expand protection rather than create procedural confusion.

Regulatory enforcement should reflect the severity and context of the breach. Relevant considerations include the sensitivity of the data, number of affected customers, duration of exposure, foreseeable harm, recurrence, quality of preventive measures, speed of containment, transparency, cooperation with authorities, and adequacy of customer remediation. An institution that conceals an incident or fails to preserve evidence should not be treated in the same manner as an institution that detects a sophisticated attack, responds promptly, assists customers, and corrects the weakness. Proportionality supports both fairness and regulatory credibility.

The supervisory coordination mechanism should begin with a clear classification matrix. A personal data breach involving a bank's internal information system requires attention from the bank, OJK, and the personal data protection supervisory institution, while a payment system incident may additionally involve Bank Indonesia. A cyber incident may trigger cybersecurity resilience reporting, while an unlawful downstream use by a Non-PJP Service User may require action directed at both the user and the service provider that failed to supervise cooperation (Amalia, 2022). A single incident may therefore require coordinated action without collapsing the distinct legal competences of each institution.

Coordination should operate through documented channels. Regulators should determine the minimum information required for incident reporting, establish procedures for forwarding matters outside their primary competence, and prevent unnecessary duplication where the same evidence is requested repeatedly. A coordinated protocol should also define when customers receive updates and which institution communicates public information in cases affecting a large number of users. Regulatory fragmentation becomes manageable when each authority understands both its own mandate and the points at which cooperation is required.

A coordinated model must also anticipate institutional failure to cooperate. Where several authorities are potentially involved, a default lead-authority approach is needed to prevent delay. As a general rule, OJK should lead where the breach primarily concerns the bank-customer relationship and consumer loss within the financial services sector, Bank Indonesia should lead where the incident primarily concerns payment system operations and Open API Payments governance, and the personal data protection supervisory institution should lead where the central issue concerns unlawful processing, data subject rights, or breach notification under the personal data protection regime. Where disagreement persists, the authority first receiving a substantiated report should remain responsible for ensuring interim customer-facing protection until inter-authority competence is resolved.

The contractual relationship among institutions must support regulatory coordination. Cooperation agreements should define data categories, processing purposes, roles, lawful bases, access methods, consent records, retention periods, security standards, audit rights, incident reporting timelines, evidence preservation duties, customer notification procedures, remediation responsibilities, regulator communication, and internal recourse. These clauses should be specific enough to guide action during an incident (Ali et al., 2026). A generic confidentiality clause is insufficient for a service involving continuous digital connectivity and sensitive financial data.

Data protection by design should become an operational principle in Open API development. Security, minimization, access control, revocation, logging, retention, deletion, and incident response should be incorporated at the architecture stage (Amalia, 2022). This approach is consistent with the high-risk nature of specific personal financial data and with the requirement to conduct impact assessments where appropriate. It is also more efficient than attempting to repair structural weaknesses after a breach has already affected customers.

The effectiveness of coordination also depends on institutional capacity. Smaller fintech entities, Non-PJP Service Users, or under-resourced complaint-handling bodies may lack the technical, forensic, or compliance capacity available to large banks and major payment providers. This asymmetry matters because a

formally equal obligation may produce unequal practical results. A coordinated protocol should therefore include minimum documentation standards, escalation timelines, and mandatory cooperation duties that prevent weaker actors from becoming blind spots within the accountability chain.

The doctrinal basis of the proposed model is legal certainty. Customers need to know which institution will respond, what information they will receive, how they may restrict further processing, and where they may seek a remedy. Business actors need to know which obligations cannot be delegated and which contractual arrangements are required for cooperation. Regulators need a coordinated basis for supervision and enforcement.

The model is also grounded in corrective justice. An institution benefiting from a digital service architecture should bear responsibility for restoring the position of a customer harmed by failures within that architecture according to its role and conduct. Corrective justice does not require every actor to bear identical consequences. It requires responsibility to follow control, fault, benefit, risk creation, and the ability to prevent or remedy harm.

The findings challenge the assumption that the existence of consent and technical standards is sufficient to protect banking customers. Consent is legally important but limited by purpose, transparency, scope, and the customer's ability to exercise rights. Technical standards reduce risk but cannot eliminate incidents or determine compensation by themselves. A complete legal framework must connect consent and standardization with responsibility, evidence, notification, remediation, and regulatory coordination.

Several regulatory improvements can operationalize the model. Bank Indonesia, OJK, and the personal data protection supervisory institution should formulate a coordinated protocol for personal data breaches involving banking and payment system services. The protocol should clarify role classification, minimum reporting content, evidence preservation, notification coordination, complaint forwarding, customer assistance, public communication, and follow-up supervision. It should also address the position of Non-PJP Service Users and cross-border processors.

The legal protection of banking customers should ultimately be evaluated through outcomes. A customer-centered system must reduce unauthorized access, identify failures promptly, provide understandable information, stop further processing, restore customer control, resolve financial losses, and correct institutional weaknesses (kumari, 2025). Compliance documents are relevant because they support these outcomes, not because they constitute an end in themselves. The law should therefore measure the effectiveness of protection through both process and result.

The integrated accountability and redress model proposed in this study consists of eight connected elements. These elements are role classification, lawful and limited data access, accountable partner governance, documented security and resilience, coordinated incident response, single-entry customer complaints, accountability-based evidence management, and proportionate remediation supported by regulatory coordination. Each element addresses a weakness identified through the normative mapping. Their integration transforms a collection of regulations into a functional structure of legal protection. Taken together, these elements are intended to function sequentially in breach cases: role identification determines the responsible actor, limited access and partner governance clarify the legality of processing, coordinated response and complaint access secure immediate protection, evidence management supports attribution, and proportionate remediation completes the corrective dimension.

The model also answers the second research question by proposing a customer-centered accountability structure. The structure does not require the elimination of specialized regulation or the imposition of identical liability on every participant. It requires an accessible response for customers, functional allocation of responsibility, preservation of evidence, timely notification, proportionate compensation, and coordination among institutions. The model places the customer at the center of legal protection while allowing internal recourse among business actors according to their respective failures.

The contribution of this analysis lies in developing a more explicit breach centered reading of Indonesia's open banking framework. Earlier discussions

have emphasized standardization, consent, and regulatory development, but they have less clearly translated those norms into an operational structure for notification, complaint access, evidence preservation, responsibility allocation, and remediation after preventive safeguards fail. The present analysis seeks to fill that doctrinal gap.

The proposed model supports the sustainable development of digital financial services in Indonesia. Legal certainty, cybersecurity resilience, consumer protection, and personal data protection are not separate policy objectives. They are interdependent conditions for building trust in an interconnected payment ecosystem. Open banking innovation will remain legitimate only when customers retain meaningful control over personal financial data and receive effective protection when that control is violated.

Cross-border processing and customer facing controls must also be incorporated into the accountability framework. Open banking infrastructure may involve cloud services, technology vendors, or affiliated entities located outside Indonesia, requiring institutions to identify data locations, safeguards, access rights, and incident-response channels before a service is launched. Data minimization should ensure that an application receives only the information necessary for its stated purpose and authorized period (Admiral & Pauck, 2023). A consent dashboard should allow customers to identify connected entities, review active permissions, and withdraw access through an accessible interface.

The effectiveness of the model also requires measurable indicators and periodic institutional evaluation. Regulators and service providers should assess detection time, containment speed, notification quality, complaint resolution, log completeness, consent integrity, remediation, and recurrence of similar incidents. Quantitative indicators should be combined with substantive judgment because formal compliance does not necessarily demonstrate adequate protection. This evaluative approach converts general obligations into a governance system capable of identifying weaknesses and improving customer remedies.

Implementation also requires institutional discipline across each participating organization. Responsible units must be clearly designated before

an incident occurs. Escalation channels must remain operational during service disruptions. Periodic internal and independent audits should test whether the protocol works consistently under practical conditions. Institutional coordination must also be supported by interoperable documentation standards. Each participating entity should retain verifiable records of consent, access, escalation, containment, and remediation. These records enable regulators to reconstruct the processing chain without shifting an excessive evidentiary burden to customers. They also support proportionate enforcement by distinguishing isolated technical failures from recurring governance weaknesses that require stronger corrective measures across the interconnected financial services ecosystem.

Conclusion

This study concludes that the protection of banking customers against personal data breaches in Indonesian open banking services is already supported by a multilayered regulatory framework, but that framework remains insufficiently integrated when a breach involves multiple institutions. The main weakness lies not in the absence of preventive regulation, but in the lack of a clear post incident structure for identifying the responsible actor, handling complaints, preserving evidence, and delivering remedies to affected customers. The contribution of this study is twofold. Theoretically it shifts the analysis of open banking protection from a consent and compliance focus toward a clearer post-incident accountability perspective. Practically, it offers a model that may guide banks, payment service providers, regulators, and complaint-handling bodies in determining who should respond first, how customer complaints should be handled, and how remedies should be coordinated when personal data protection fails.

This study is limited by its normative design and therefore does not test how the proposed model operates in actual institutional practice. The most urgent empirical questions for future research are whether banks and other customer-facing institutions in fact assume immediate responsibility after a breach, and whether a single-entry complaint mechanism can function effectively across

overlapping supervisory and contractual relationships in the open banking ecosystem. Empirical investigation should therefore focus on post-incident practice within banks, payment service providers, Non-PJP partners, regulators, and dispute resolution bodies, particularly in relation to first response, evidence access, interim customer protection, and the coordination of final remedies.

References

Adedoyin Tolulope Oyewole, Bisola Beatrice Oguejiofor, Nkechi Emmanuella Eneh, Chidiogo Uzoamaka Akpuokwe, & Seun Solomon Bakare. (2024). Data Privacy Laws And Their Impact On Financial Technology Companies: A Review. *Computer Science & IT Research Journal*, *5*(3), 628–650. https://doi.org/10.51594/csitrj.v5i3.911

Admiral, A., & Pauck, M. A. (2023). Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services. *Lex Scientia Law Review*, *7*(2), 995–1048. https://doi.org/10.15294/lesrev.v7i2.77881

Agustianto, A., Sacramed, M. T., Fitri, W., Weley, N. C., & Disemadi, H. S. (2026). Regulatory Gaps in Data Protection and Proportionality in Digital Banking: Legal Issues in ASEAN. *Syura: Journal of Law,* 4(1), 55-86. https://doi.org/10.58223/syura.v4i1.811

Algamar, M. D., Munir, A. B., & Hendro. (2024). Managing Indonesian Data Breach Notification In The Financial Services Sector: A Case For One-Stop Notification Model. *Journal of Central Banking Law and Institutions*, *3*(3), 547–584. https://doi.org/10.21098/jcli.v3i3.271

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2026). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*, *66*(1), 123–150. https://doi.org/10.1080/08874417.2024.2329985

Alkhamsi, N. N., & Alqahtani, S. S. (2024). Compliance Framework for Personal Data Protection Law Standards. *International Journal of Advanced Computer Science and Applications*, *15*(7). https://doi.org/10.14569/IJACSA.2024.0150751

Amalia, C. (2022). Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment. *Journal of Central Banking Law and Institutions*, *1*(2). https://doi.org/10.21098/jcli.v1i2.19

Amirulloh, M., Handayani, T., & Sadam, A. V. (2025). Keamanan Siber (Cybersecurity) pada Sistem Perbankan Digital di Indonesia Berdasarkan Hukum Siber Indonesia. *Jurnal Inovasi Global*, *3*(5), 718–727. https://doi.org/10.58344/jig.v3i5.323

Amboro, Y. P., Macnico, P., Tan, W., & Bajury, M. S. M. (2025). Digital Democracy and Open Finance Technology: Advancing Transparency and Consumer Digital Rights. *Lex Publica,* 12(2), 331-360. https://doi.org/10.58829/lp.12.2.2025.295

Anderson-Princen, J. M. (2022). Cloud Outsourcing in the Financial Sector: An Assessment of Internal Governance Strategies on a Cloud Transaction Between a Bank and a Leading Cloud Service Provider. *European Business Organization Law Review*, *23*(4), 905–936. https://doi.org/10.1007/s40804-022-00252-4

Bella Fistya Asherli, & Sidi Ahyar Wiraguna. (2025). Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022. *Jurnal Hukum, Administrasi Publik Dan Negara*, *2*(4), 01–14. https://doi.org/10.62383/hukum.v2i4.290

Billiam, B., Abubakar, L., & Handayani, T. (2022). The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *9*(1), 67–88. https://doi.org/10.22304/pjih.v9n1.a4

Dahi, A., & Compagnucci, M. C. (2022). Device manufacturers as controllers – Expanding the concept of 'controllership' in the GDPR. *Computer Law & Security Review*, *47*, 105762. https://doi.org/10.1016/j.clsr.2022.105762

Diyanatalia, J. L., Sudirman, L., & Disemadi, H. S. (2025). Pengawasan Otoritas Jasa Keuangan Dan Dampaknya Terhadap Efektivitas Perlindungan Data Konsumen Bank Perekonomian Rakyat Di Batam. J*urnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat,* 11(3), 546-571. https://doi.org/10.55809/tora.v11i3.592

Florence Olweny. (2024). Navigating the nexus of security and privacy in modern financial technologies. *GSC Advanced Research and Reviews*, *18*(2), 167–197. https://doi.org/10.30574/gscarr.2024.18.2.0043

Ghosh, A., Mukhopadhyay, I., & Chakraborty, S. (2023). ConsenTrack-Blockchain Based Framework for Open Banking Consent Data Tracking. *Human-Centric Intelligent Systems*, *3*(2), 105–122. https://doi.org/10.1007/s44230-023-00023-5

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.1016/j.eswa.2023.122697

Karthika M., Neethu K., & Lakshmi P. (2022). Impact of Fintech on the Banking Sector. *Integrated Journal for Research in Arts and Humanities*, *2*(4), 109–112. https://doi.org/10.55544/ijrah.2.4.66

Karwati, K., Hardyansah, R., & Saktiawan, P. (2024). Legal Analysis of Open Banking and Bank Customer Data Privacy Rights in Indonesia. *Journal of Social Science Studies*, *4*(1), 93–104. https://jos3journals.id/index.php/jos3/article/view/295

kumari, sonam. (2025). Adaptive Security for Digital Finance: Balancing Innovation, Risk, and Customer Experience. *International Journal For Multidisciplinary Research*, *7*(5). https://doi.org/10.36948/ijfmr.2025.v07i05.55438

Li, S. (2023). Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. *Maastricht Journal of European and Comparative Law*, *30*(3), 335–345. https://doi.org/10.1177/1023263X231208835

Librawenson, W., Disemadi, H. S., & Afdal, W. (2025). Regulating the Right to Be Forgotten in Indonesia's Digital Banking: Lessons from the EU GDPR. *Jurnal Mediasas: Media Ilmu Syari'ah dan Ahwal Al-Syakhsiyyah*, *8*(4), 1008-1028. https://doi.org/10.58824/mediasas.v8i4.501

Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets*, *31*(4), 829–848. https://doi.org/10.1007/s12525-021-00490-3

Modesti, P., Freitas, L., Shotomiwa, Q., & Almehrej, A. (2025). Security analysis of the open banking account and transaction API protocol. *Cyber Security and Applications*, *3*, 100097. https://doi.org/10.1016/j.csa.2025.100097

Naudts, L., Dewitte, P., & Ausloos, J. (2022). Meaningful transparency through data rights: A multidimensional analysis. In *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing. https://doi.org/10.4337/9781800371682.00030

Nuredini, B., Xhafaj, J., & Paukovska Dodevska, V. (2022). A Comparative Overview of Data Protection in e-Commerce in the European Union, the United States of America, the Republic of North Macedonia, and Albania: Models and Specifics. *Studia Iuridica Lublinensia*, *31*(3), 61–84. https://doi.org/10.17951/sil.2022.31.3.61-84

Nurlaily, N., Sudirman, L., Bajury, M. S. M., Disemadi, H., & Silviani, N. (2025). Digital Advertising as a Threat to Consumer Privacy: A Comparative Legal Analysis. *QONUN: Jurnal Hukum Islam Dan Perundang-Undangan,* 9(2), 359-388. https://doi.org/10.21093/qj.v9i2.12656

Pati, U. K., & Pratama, A. M. (2025). Indonesia's Open Banking Future: Designing Effective Regulatory Approaches. *Jambe Law Journal*, *8*(1), 27–60. https://doi.org/10.22437/home.v8i1.371

Purwanti, N., Barthos, M., & Saputra, T. E. (2025). The Role of Artificial Intelligence in the Implementation of Personal Data Protection Law in Indonesia. *Interdiciplinary Journal and Hummanity (INJURITY)*, *4*(6), 325–336. https://doi.org/10.58631/injurity.v4i6.1448

Rannie B., W. (2023). Legal Protection of Customer Personal Data in the Banking Sector. *ARRUS Journal of Social Sciences and Humanities*, *3*(5), 710–717. https://doi.org/10.35877/soshum2169

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. https://doi.org/10.1093/cybsec/tyw001

Sakti, M., Utami, K., & Sulastri. (2024). The Urgency Of Standardizing The Open Application Programming Interface In Implementation Of Open Banking For Customer Protection. *Jurnal Hukum Samudra Keadilan*, *19*(1), 29–44. https://doi.org/10.33059/jhsk.v19i1.7471

Saputra, T. E. (2024). Penggunaan Rekam Medis Elektronik dalam Mewujudkan Perlindungan Hukum Keamanan Data Pribadi Pasien. *Fundamental:*

Jurnal Ilmiah Hukum, *13*(2), 57–75. https://doi.org/10.34304/jf.v13i2.276

Sari, N. (2023). Accelerating Business Law Dynamization through Proposed Amendments to Indonesian Consumer Protection Law. *Jurnal Hukum Novelty*, *14*(1), 88. https://doi.org/10.26555/novelty.v14i1.a25945

Sarif, A., & Ariyanti, R. (2024). The Innovation of Digital Payment System with QRIS in National Open API and Maqasid al-Sharia Standards. *International Journal of Applied Business and International Management*, *9*(2), 96–114. https://doi.org/10.32535/ijabim.v9i2.2553

Situmeang, A., Disemadi, H. S., & Marsudi, I. R. (2024). Contextualizing Consumer Data Protection within the Operational Principles of Banking: A Legal Inquiry. *Legal Spirit,* 8, 365-78. https://doi.org/10.31328/ls.v8i2.5458

Sudirman, L., Disemadi, H. S., & Aninda, A. M. (2023). Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective. *JED (Jurnal Etika Demokrasi)*, *8*(4), 497–510. https://doi.org/10.26618/jed.v8i4.12875

Syailendra, M. R. (2024). Personal Data Protection Law In Indonesia: Challenges And Opportunities. *Indonesia Law Review*, *14*(2). https://doi.org/10.15742/ilrev.v14n2.4

Taufiq, M. (2025). Dispute Resolution in Consumer Protection in the Financial Services Sector Perspective Sadd al-Zari'ah. *Al-Mustashfa: Jurnal Penelitian Hukum Ekonomi Syariah*, *10*(1), 76. https://doi.org/10.24235/jm.v10i1.19570

Thomas, G., & Sule, M.-J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1), 18–40. https://doi.org/10.1108/OCJ-09-2021-0025

van Zeeland, I., & Pierson, J. (2024). Changing the whole game: effects of the COVID-19 pandemic's accelerated digitalization on European bank staff's data protection capabilities. *Financial Innovation*, *10*(1), 29. https://doi.org/10.1186/s40854-023-00533-y

Wolters, P. T. J., & Jacobs, B. P. F. (2019). The security of access to accounts under the PSD2. *Computer Law & Security Review*, *35*(1), 29–41. https://doi.org/10.1016/j.clsr.2018.10.005

Zachariadis, M., & Ozcan, P. (2016). The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2975199

Zeynalova, A. (2024). From Closed Banking to Open Banking: Risks and Opportunities. *Journal of Applied Business, Taxation and Economics Research*, *3*(3), 303–316. https://doi.org/10.54408/jabter.v3i3.278

Acknowledgments

The author extends sincere gratitude to their academic supervisor and Universitas Dr. Soetomo for the academic support provided during the preparation of this article. This article is submitted as a partial fulfillment of the requirements for the degree of Bachelor of Laws at Universitas Dr. Soetomo.

Declaration of Generative AI Use

The author(s) declare that no generative AI or AI-assisted technologies were used in the preparation or writing of this manuscript. All content was produced entirely by the author(s) without any automated assistance.

Competing Interest

There is no conflict of interest in the publication of this article.

This page intentionally left blank

ISSN (Print) 1907-6479 | ISSN (Online) 2774-5414