



DISPUTE RESOLUTION IN DIGITAL BANKING ARISING FROM BIOMETRIC AUTHENTICATION: A COMPARATIVE STUDY OF INDONESIA AND SINGAPORE

Suwandi

Master of Law Program, UPN "Veteran" Jawa Timur, Indonesia

Suwandi.fh05@gmail.com

Teddy Prima Anggriawan

Master of Law Program, UPN "Veteran" Jawa Timur, Indonesia

teddyprima.ih@upnjatim.ac.id

Abstract: This article examines digital banking disputes arising from biometric authentication in mobile banking, including authentication failures, misuse of biometric data, and bank liability for customer losses. It compares the legal frameworks of Indonesia and Singapore, two countries pursuing financial digitalization with different approaches to consumer and personal data protection. The study uses a normative juridical method with statutory and comparative approaches. The findings indicate that Indonesia has a basic legal framework comprising the Electronic Information and Transactions Law, the Personal Data Protection Law, and Financial Services Authority regulations. However, clearer evidentiary and liability standards and more consistent compensation procedures are needed for biometric-related disputes. Singapore offers a more structured framework through its personal data protection legislation, electronic payments user-protection guidelines, and dispute-resolution arrangements administered by FIDReC. The comparison highlights the importance of security governance, transparent investigations, and accessible dispute resolution in protecting customers.

Keywords: digital banking, biometric authentication, customer protection, LAPS SJK, FIDReC.

INTRODUCTION

The migration of banking services from face-to-face to digital channels has transformed how banks create legal relationships with consumers. Banking apps, internet banking, and online account opening increase banking efficiency but shift the risk exposure from the physical area to cyberspace. In this context, what were mostly administrative difficulties in banking disputes are now increasingly being replaced by faults in electronic systems, aside from credential theft, takeovers of accounts, and unauthorized access due to deficiencies in authentication

measures. Hence, a change in risk characteristics requires a recalibration of bank accountability and evidentiary models relevant to electronic transactions (Rosadi, 2023).

Biometric authentication is an industry response to the rise of attacks based on passwords and one-time passwords. Biometric authentication is the use of a user's physiological or behavioral attributes like fingerprints, face, iris, or keystroke patterns to authenticate identity. In mobile banking, biometrics are generally seen as a better layer of protection than a PIN because they are difficult to duplicate and can be integrated with device security. Nevertheless,

biometrics are non-standard "keys" in that they are permanently linked to the body and cannot be replaced once they have been compromised. Biometric systems are also susceptible to false acceptance (accepting the wrong person) and false rejection (rejecting the right person) risks, which can adversely affect customers and tarnish banks' reputations (Palindria et al., 2024).

Biometric data is a special category of personal data, which is specially protected in the legal system. The Personal Data Protection Law explicitly states that the processing of some personal data needs to be based on a stricter legal foundation, a precautionary approach, and appropriate security measures (Rosadi, 2023). A bank that needs or supports biometric authentication also becomes a data controller/processor with security and compliance duties. Failure to perform these commitments may lead to civil liability and to administrative or even criminal liability, depending on the nature of the breach and its consequences.

Singapore is a useful comparator in that it has a relatively established digital identity ecosystem and well-structured electronic payments user protection mechanisms. The PDPA in Singapore sets out basic criteria for the acquisition, use, and disclosure of personal data by organizations (Personal Data Protection Act, 2012). In the field of electronic payments, the Monetary Authority of Singapore (MAS) issued the E-Payments User Protection Guidelines, which outline the duties of banks and users in cases of unauthorized transactions (Monetary Authority of Singapore, 2020). Further, the Financial Industry Disputes Resolution Centre (FIDReC),

as an independent ADR agency, generally accepts consumer financial issues (Financial Industry Disputes Resolution Centre Ltd., 2026). The framework demonstrates the contribution of the design of norms and institutions to effecting the certainty of loss recovery.

Against this background, this study seeks to clarify compliance standards and bank obligations concerning biometric authentication. Without clear standards, disputes may become competing narratives: banks may assert that a transaction was authenticated, while customers may allege coercion, social engineering, or system failures. Information and technical asymmetries can disadvantage customers who must demonstrate that a security failure was not attributable to their own conduct (Antono & Saputra, 2025). This study therefore offers conceptual analysis and policy recommendations on security regulation, evidence concerning biometric incidents, and the effectiveness of dispute-resolution forums in Indonesia, drawing lessons from Singapore.

The literature on digital banking in Indonesia tends to focus on cybercrime risks, bank secrecy, and consumer protection through OJK supervision. Research connecting biometric authentication specifically with liability models and dispute-resolution design remains limited. Biometrics operate alongside device registration, token management, and transaction limits. In a dispute, these arrangements affect whether a failure is attributed to system weaknesses, customer negligence, or a third-party attack.

A legal approach that relies solely on standard terms and conditions may

overlook good faith and contractual balance. Banks commonly use limitation-of-liability clauses, while customers have limited scope to negotiate. Dispute-resolution forums should therefore scrutinize clauses invoked to exclude banks' security obligations as electronic system operators. POJK No. 22 of 2023 on Consumer and Public Protection in the Financial Services Sector establishes principles of transparency, fair treatment, and adequate complaint handling. Its relevance to biometric disputes lies in complaint-service standards and information disclosure obligations (Antono & Saputra, 2025).

RESEARCH QUESTIONS

This study addresses five questions: (1) What is the role of biometric authentication in digital banking, and what legal risks does it present? (2) What disputes arise from biometric authentication, and what are the respective legal positions of banks and customers? (3) How do Indonesia's regulatory and dispute-resolution mechanisms operate, including LAPS SJK? (4) How do Singapore's comparable arrangements operate under the PDPA, MAS guidelines, and FIDReC? (5) What lessons can strengthen legal certainty and customer protection in Indonesia?

RESEARCH METHOD

This study uses a normative juridical method with statutory, conceptual, and comparative approaches. Primary legal materials comprise legislation and relevant regulatory guidelines from Indonesia and Singapore. Secondary materials include academic literature on digital banking and data protection. Materials

were collected through library research covering legislation, OJK guidelines, MAS publications, and academic literature indexed in SINTA 3–4. Qualitative analysis examines normative consistency, the allocation of responsibility, and the institutional effectiveness of dispute resolution to develop recommendations for Indonesia.

To make the comparison possible, the study deals with two variables: (a) the design of liability and the burden of proof in disputed transactions, and (b) the efficiency of ADR forums in restoring consumer losses. The first variable is analyzed through the norms and operational standards and the second through the procedural framework, the accessibility, and the forum's ability to deal with electronic evidence.

RESULTS AND DISCUSSION

The Concept of Biometric Authentication in Digital Banking Services

Biometric authentication is the process of identifying a person based on their unique characteristics. Biometrics are commonly utilized for mobile banking services in two phases: (a) access to the application (login) and (b) authorization of transactions over specific amounts. In terms of information security, biometrics are generally paired with a possession factor (registered device) and a knowledge factor (PIN) to create multi-factor authentication.

Common biometric modalities include fingerprints and facial recognition. In more recent developments, some banks also use behavioral biometrics to detect transaction anomalies, such as screen

touch patterns or indications that the user is on a phone call while making a transfer—features that, in many cases, are associated with social-engineering fraud (Monetary Authority of Singapore, 2023).

From the standpoint of privacy law, biometric data is specific personal data because it can uniquely identify an individual. Consequently, data controllers must apply data minimization, purpose limitation, and security measures proportionate to the risk. Biometric risk is distinctive due to irreversibility: once biometric templates are exposed, individuals cannot “change” their face or fingerprints the way they change a password. Deepfake threats and AI-based facial spoofing further reinforce the urgency of biometric safeguards and liveness verification (Palindria et al., 2024).

In the bank–customer relationship, biometric authentication forms part of the bank’s duty of care in providing electronic services. This duty extends beyond installing an authentication feature. It includes secure design, customer risk education, controls over device activation, and transparent incident management to ensure that biometric authentication protects customers rather than merely transferring risk to them.

From a contract-law perspective, biometric authentication is also used to express consent in electronic contracts. Questions remain about its legal status and its relationship to electronic signatures and other forms of consent. Regulatory harmonization is therefore needed to reduce uncertainty in disputes (Sabila et al., 2025).

From a technical perspective, biometric systems should ideally use

processed and encrypted templates rather than retain raw images unnecessarily. Some architectures use secure enclaves or trusted execution environments so that biometric data remain on the device. Others require server-side processing, such as identity verification during account opening. These design choices have different legal implications: the more biometric data a bank processes, the greater its compliance responsibilities as a data controller.

Consent presents a further issue. A one-click agreement in an application’s settings should be assessed to determine whether it provides specific and informed consent. Banks should explain the purposes of biometric processing, retention periods, any recipients of the data, and how consent may be withdrawn without unnecessarily restricting access to essential services.

Biometric authentication must also be considered within operational risk management. Banks need procedures for prevention, detection, and incident response. In biometric incidents, these include promptly disabling compromised authentication, restoring access for locked-out customers, and conducting forensic investigations while preserving the integrity of electronic evidence. Without such procedures, biometric authentication may compound losses by delaying recovery.

Digital Banking Disputes Arising from the Use of Biometric Authentication

Digital banking disputes often begin with a contested transfer, an unauthorized change to transaction

limits, or the activation of an unfamiliar device. Biometric disputes can be grouped into three categories: (a) false rejections or other authentication failures that deny customers access and cause lost opportunities; (b) false acceptances or authentication by unauthorized parties that result in financial loss; and (c) misuse of biometric data or processing without a lawful basis.

A central legal question is whether a transaction is valid merely because the system recorded successful biometric authentication. An authentication log does not necessarily establish voluntary customer consent. Social-engineering victims may authorize transactions under pressure or surrender control of their devices through remote-access applications. If evidentiary standards disregard this context, biometric records may become a one-sided justification for rejecting customer complaints.

Biometric disputes also involve information asymmetry. Banks control system logs, security parameters, and activity records, while customers may have only notifications and their own accounts of events. This disparity can strengthen banks' negotiating position. Evidentiary standards should therefore require proportionate technical disclosure, including log summaries, device-activation timelines, and verifiable investigation findings.

Risk allocation is central to consumer protection. Assigning all losses to customers would disregard possible system failures, while assigning all losses to banks would overlook customers' contribution to an incident. A balanced framework should assess whether the bank implemented

reasonable controls and whether the customer exercised reasonable care.

Successful authentication can occur during phishing-related account takeovers. Victims may be induced to disclose credentials, activate a device, or authorize a transaction. Although the victim completes the biometric check, consent may be affected by misinformation or pressure. Dispute assessment should therefore consider not only authentication logs but also risk warnings, waiting periods, and restrictions on high-risk changes.

Banks are generally better placed to produce electronic evidence because they hold technical records such as device-registration times, IP addresses, geolocation, device models, and transaction histories. Proportionate disclosure of these records can support a fair assessment of whether anti-fraud controls should have detected an anomalous transaction.

Losses in biometric disputes may extend beyond missing funds to recovery costs, lost business opportunities, and distress resulting from account lockout or data exposure. Compensation assessment should therefore consider reasonable recovery expenses and any legally recoverable non-financial harm, particularly where a system weakness contributed to the incident.

Legal Regulation and Digital Banking Dispute Resolution in Indonesia

In Indonesia, digital banking services are based on the combination of banking norms, norms of electronic transactions, and norms of personal data security. Institutionally, the Financial Services Authority (OJK) has a responsibility in prudential regulation

and supervision, as well as consumer protection. Moreover, the Personal Data Protection Law introduces wider controller compliance obligations, including for banks when processing the biometric data of customers (Rosadi, 2023).

Where biometric authentication forms part of an electronic system, system failure or a data breach may have liability implications for the bank. Relevant duties include maintaining reliable, secure, and accountable electronic systems and complying with consumer-protection requirements concerning service safety and accurate information.

Dispute resolution generally begins with the bank's internal complaint process. If no agreement is reached, the customer may seek alternative dispute resolution through LAPS SJK under POJK No. 61/POJK.07/2020 (Otoritas Jasa Keuangan, n.d.). LAPS SJK offers a confidential alternative to litigation, with mediation oriented toward an agreed settlement (Ginting & Lubis, 2025). Its effectiveness nevertheless depends on consumer awareness and consistent procedures. In biometric disputes, complex technical evidence can impede mediation when evidentiary standards and access to relevant records are inadequate.

Court proceedings remain an option, although litigation may require substantial time, expense, and technical expertise. Alternative dispute-resolution mechanisms should therefore be equipped to assess electronic evidence through log analysis, independent security audits, and proportionate disclosure in biometric-related disputes.

One of the most frequently mentioned instruments in electronic

transaction disputes is the ITE Law and its revisions. ITE Law recognizes electronic evidence and requires electronic system operators to maintain dependable and secure systems. These rules are the foundation upon which the basic security standards banks are to adhere to when offering mobile banking, which includes biometric authentication, will be measured in disputes.

The Personal Data Protection Law introduces a new dimension by defining biometric data as special personal data. Therefore, banks are required to have appropriate security measures in place, to perform impact assessments where necessary, and to have protocols for dealing with data breaches. Compliance with the Personal Data Protection Law may be used as a yardstick in a dispute to assess whether the bank used due care.

OJK regulations on digital banks and consumer protection increase the banks' responsibilities to make sure that complaint procedures are clear, accessible, and within the resolution time limits. POJK 22/2023 highlights the importance of fair treatment and reliable complaint services (Antono & Saputra, 2025). In illicit transactions, response speed is typically the determinant of how much loss occurs, as monies can be quickly moved through mule accounts.

Access to LAPS SJK is linked to prior internal complaint handling. A customer ordinarily submits a complaint to the bank for explanation and investigation before seeking external resolution. Ginting and Lubis (2025) describe procedures ranging from administrative screening to mediation and, in applicable

proceedings, binding outcomes. Clear procedural information helps customers understand their available routes to recovery.

Inconsistent evidentiary and investigative practices can create uncertainty. Some banks provide log summaries and timelines, while others rely on a general statement that the transaction was authenticated. Such differences can lead dissatisfied customers to seek public attention through social media and may undermine trust in the industry.

To address these barriers, OJK and LAPS SJK should establish minimum evidentiary standards. These could specify the information banks must disclose, response timeframes, and procedures for verifying customers' identities when biometric access is disabled. Clear standards would help dispute-resolution proceedings focus on substantive compliance and the causes of an incident.

Legal Regulation and Digital Banking Dispute Resolution in Singapore

In Singapore, the processing of personal data is governed by the Personal Data Protection Act 2012 (PDPA) which lays down organizational obligations for the collection, use, disclosure, and protection of personal data (Personal Data Protection Act, 2012). As the competent body, the PDPC provides compliance assistance and stresses that the PDPA is intended to complement sectoral frameworks such as the Banking Act (PDPC Singapore, 2025). With regard to biometrics, the requirements of protection and purpose limitation are key to the analysis of the bank's compliance.

In electronic payments, the MAS issued the E-Payments User Protection Guidelines, which prescribe the roles of account holders and payment service providers in the event of unauthorized transactions, such as quick reporting duties, investigation, and loss reimbursement mechanisms under certain conditions (Monetary Authority of Singapore, 2020). The guidelines are designed to make the allocation of responsibility more operational and to use technical standards to reduce arguments about "who bears the loss."

Biometric controls are also included in the national digital identity infrastructure. On 18 September 2024, the Association of Banks in Singapore announced that retail banks will deploy Singpass Face Verification to strengthen digital token activation, especially in high-risk phishing cases (Association of Banks in Singapore, 2024). This development points to a move to biometrics not just for login but as process controls to prevent account takeover from new devices.

FIDReC is an independent institution offering mediation and adjudication of consumer disputes with financial institutions (Financial Industry Disputes Resolution Centre Ltd., 2026). Its specialized procedures provide an accessible route for seeking redress without immediately resorting to litigation.

Singapore's PDPA establishes consent and purpose-limitation requirements, subject to applicable exceptions. Banks should therefore define the purposes of biometric processing and limit processing to what is necessary. The PDPC describes the PDPA as a baseline framework that complements sectoral

legislation, including the Banking Act (PDPC Singapore, 2025).

The MAS E-Payments User Protection Guidelines set out user responsibilities, including safeguarding credentials and reporting unauthorized transactions, alongside financial institutions' investigation and recovery duties. These requirements help focus disputes on factual questions concerning customer conduct and the adequacy of institutional controls (Monetary Authority of Singapore, 2020).

Singapore has also strengthened controls over device activation. Singpass Face Verification checks identity against national records in relevant high-risk scenarios and is used during digital token activation (Association of Banks in Singapore, 2024). This approach targets a stage that can be exploited in account-takeover attacks.

FIDReC provides procedures for complaint submission, early resolution, mediation, and, where necessary, adjudication. This offers consumers a specialized alternative to litigation and can reduce the costs of pursuing redress (Financial Industry Disputes Resolution Centre Ltd., 2026).

Comparison of Digital Banking Dispute Resolution in Indonesia and Singapore

The main distinction concerns how responsibility is translated into operational requirements. Indonesia has a broad legal framework, but evidentiary requirements and the allocation of losses leave room for interpretation. Singapore provides more detailed guidance on the responsibilities of users and financial

institutions, including investigation and recovery procedures.

LAPS SJK and FIDReC both provide alternative dispute resolution in the financial sector. FIDReC uses established mediation and adjudication procedures, while Indonesian scholarship identifies a need to improve access and procedural capacity within LAPS SJK. Technical evidence in digital banking disputes makes these institutional capacities particularly important (Ginting & Lubis, 2025).

Both jurisdictions recognize the importance of protecting biometric data. Singapore links some biometric controls to its national digital identity infrastructure, whereas Indonesian practices rely more heavily on device-level authentication and individual banks' arrangements. Consequently, protection against spoofing, deepfakes, and social-engineering attacks may vary across Indonesian banks.

The comparison indicates that customer protection depends not only on biometric features but also on security governance, transparent investigations, and dispute-resolution forums capable of assessing electronic evidence.

Clear allocation of duties can facilitate the assessment of disputed transactions. Defined standards for customer conduct and bank controls help mediators and adjudicators evaluate liability and possible compensation. Broadly formulated duties, by contrast, may leave disputes focused on abstract legal arguments rather than the evidence.

Indonesia can strengthen controls at high-risk stages, particularly new-device registration and changes to registered telephone numbers.

Liveness checks, restrictions on changes to transaction limits, and repeated notifications may help prevent losses. Singapore also faces evolving fraud and deepfake threats, demonstrating the continuing need for coordination among banks, regulators, and digital identity providers, supported by broader anti-fraud measures.

Legal Implications for Legal Certainty and Customer Protection

First, Indonesia needs clearer minimum standards for biometric security and incident evidence. These should address device activation, facial liveness checks, and cooling-off periods for high-risk changes such as registering new devices or increasing transaction limits. Singapore's use of Singpass Face Verification illustrates the importance of controls at the setup stage (Association of Banks in Singapore, 2024).

Second, complaint management methods should respect the idea of limited disclosure. Banks are required to provide a summary of a verifiable inquiry, including a technical chronology, without revealing key system secrets. Such transparency is important to eliminate information asymmetry and to promote trust in complaint outcomes.

Third, LAPS SJK should strengthen its capacity to handle technically complex disputes. Possible measures include digital-forensics expertise, procedures for examining electronic evidence, and minimum documentation requirements for banks. Alternative dispute resolution should assess security compliance and incident causes as well as negotiate financial settlements.

Fourth, banks should adopt privacy by design and data minimization, including limited retention of biometric templates, strong encryption, and periodic audits. Biometric processing should remain proportionate and be supported by safeguards against deepfakes and spoofing (Palindria et al., 2024).

Fifth, measurable consumer education is a critical component. Education should not be generic; it should target danger points such as restrictions on sharing OTPs, prohibitions on installing remote-access applications, and how to validate calls claiming to be from the bank. Measurable education can be used as an assessment criterion in measuring the user's contribution to negligence.

Sixth, authentication change management should be regulated. If biometrics are deactivated due to a dispute, banks must offer secure alternative authentication and not leave consumers without access for long periods. These procedures must address the needs of victims to recover while preventing perpetrators from utilizing avenues of recovery to take over accounts.

Seventh, effective independent supervision of personal data protection is needed to strengthen oversight of biometric processing. Audits and enforcement should support preventive compliance so that civil disputes are not the sole means of correcting failures.

CONCLUSION

Biometric authentication can improve mobile banking security but also creates distinctive risks, including false acceptances, false rejections, and the difficulty of replacing

compromised biometric characteristics. Liability assessment should therefore consider consent, device-activation controls, and incident management rather than rely solely on a successful authentication record. Indonesia has a basic framework spanning financial regulation, electronic transactions, consumer protection, and personal data protection. Clearer evidentiary standards, proportionate technical disclosure, and consistent recovery procedures are nevertheless needed. LAPS SJK should be supported by electronic-evidence standards and technical expertise to assess complex disputes fairly.

Singapore's experience suggests that operational guidance on bank and user duties, biometric controls at high-risk stages, and specialized dispute-resolution procedures can improve certainty in digital banking disputes. Priorities for Indonesia include clearer security duties during device activation and transaction authorization, stronger biometric data protection through privacy by design, and greater capacity for transparent assessment of electronic evidence. Future research should examine decisions and mediation outcomes to assess evidentiary practice and consistency in loss recovery, alongside the role of independent security audits.

REFERENCES

- [1] Antono, V. Y., & Saputra, A. (2025). Financial Services Authority In Consumer And Public Protection On Online Loan Based On Financial Services Authority Regulation (POJK) Number 22 Of 2023. *Jurnal Meta-Yuridis*, 8(2), 78–92.
- [2] Association of Banks in Singapore. (2024). Major Retail Banks To Introduce Singpass Face Verification, Further Strengthening Resilience Against Phishing Scams. Singapore.
- [3] Financial Industry Disputes Resolution Centre Ltd. (2026). FIDReC: Independent And Impartial Dispute Resolution Institution. FIDReC.
- [4] Ginting, M. B., & Lubis, A. A. (2025). Kajian Hukum Terhadap Prinsip Efisiensi Dan Efektivitas Penyelesaian Sengketa Konsumen Melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan Berdasarkan POJK Nomor 61/POJK.07/2020. *Juncto: Jurnal Ilmiah Hukum*, 7(2), 275–283.
- [5] Monetary Authority of Singapore. (2020). E-Payments User Protection Guidelines (with effect from 5 September 2020). Singapore.
- [6] Monetary Authority of Singapore. (2023). Submissions To Consultation Paper On E-Payments User Protection Guidelines (Annex B). Singapore.
- [7] Otoritas Jasa Keuangan. (n.d.). Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan. <https://ojk.go.id/id/kanal/edukasi-dan-perlindungan-konsumen/Pages/lembaga-alternatif-penyelesaian-sengketa.aspx>

- [8] Palindria, A. E., Thufail, M. S., & Febrian, M. R. (2024). Ancaman Deepfake Buatan Ai Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia. *Spektrum Hukum*, 21(2), 110–121. <https://doi.org/10.56444/sh.v21i2.5319>
- [9] PDPC Singapore. (2025). PDPA Overview: The Legislation And Baseline Standard Of Protection For Personal Data In Singapore. Personal Data Protection Commission.
- [10] Personal Data Protection Act. (2012). Personal Data Protection Act 2012 (Singapore) (2021 revised ed.).
- [11] Pramesti, M., Njatrijani, R., & Widanarti, H. (2025). Perlindungan Konsumen Dalam Penyelesaian Sengketa Sektor Keuangan (Studi Komparatif Laps-Sjk Dan Bpsk). *Law, Development And Justice Review*, 8(1), 52–68. <https://doi.org/10.14710/ldjr.8.2025.52-68>
- [12] Rosadi, S. D. (2023). Pembahasan Uu Pelindungan Data Pribadi (Uu Ri No. 27 Tahun 2022). Jakarta: Sinar Grafika.
- [13] Sabila, R., Widiyaningsih, W., & Zuraidah. (2025). Legal Certainty Of Biometric-Based Electronic Contracts Under Indonesian Contract Law. *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, 12(2), 383–396. <https://doi.org/10.24252/jurisprudentie.v12i2.64393>