JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i6

The Liability of Digital Banks for Data Breaches Occurring in Account Linkage

Suvarna Prajna Pattra[1*], Shelly Kurniawan[2]
[1] Program Studi Ilmu Hulum, Fakultas Hukum dan Bisnis Digital, Universitas Kristen Maranatha, Bandung, Indonesia, suvarnaprajna566@gmail.com
[2] Program Studi Ilmu Hulum, Fakultas Hukum dan Bisnis Digital, Universitas Kristen Maranatha, Bandung, Indonesia, shellyelviraa@gmail.com

[*]Corresponding Author: suvarnaprajna566@gmail.com

Abstract: The rapid growth of the digital banking sector in Indonesia has introduced innovative services such as Account Linkage, which enables customers to conduct transactions through partner platforms. While this feature enhances banking convenience, it also raises significant concerns regarding data privacy and legal accountability in the event of a data breach. This study aims to analyze the adequacy of existing legal frameworks in regulating data protection within Account Linkage services and to determine whether current Indonesian laws provide sufficient legal certainty. Employing a normative juridical research method, the research reviews statutory regulations, financial authority policies, and relevant contractual agreements. The findings indicate inconsistencies between banking law, financial service regulations, and privacy policies concerning the allocation of liability for data breaches. Moreover, the absence of a specific regulation governing Account Linkage contributes to legal ambiguity, placing consumers at greater risk and complicating the accountability of financial service providers. This study concludes that a more robust and comprehensive legal framework is urgently needed to ensure consumer protection, clarify the responsibilities of digital banks, and support fair and transparent financial innovation.

Keyword: Account Linkage, Digital Banking, Data Protection

INTRODUCTION

Currently, technology continues to advance and offers opportunities for the development of applications aimed at facilitating human activities. Technological progress and the ease of using applications are evident across various sectors of life, including the banking sector. One significant impact of technological advancement is the emergence of digital banking. Digital banking refers to banking services that enable customers to perform transactions without the need for a physical branch, utilizing digital devices instead. Although digital banking has grown rapidly, it still lacks specific regulatory frameworks. However, legal protection for digital banking services is currently governed by the Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks (Simatupang et al., 2024).

Referring to the Financial Services Authority Regulation Number 12/POJK.03/2021, Article 1, Point 22 defines a Digital Bank as "an Indonesian legal entity bank that provides and conducts its business activities primarily through electronic channels without physical offices other than the head office or by using limited physical offices." In addition, the implementation of digital banking practices in Indonesia still refers to the provisions of Law Number 10 of 1998 concerning Commercial Banking, which amended Law Number 7 of 1992 (hereinafter referred to as the Banking Law). Digital banking first emerged in Indonesia in 2016 and has continued to develop since then. Digital banking services in Indonesia are offered by various companies operating in the financial services sector, integrating financial services with technology in their banking practices (Purwanto, 2022).

The growth of digital banking has introduced several distinctions compared to conventional banking, particularly in the way services are delivered to customers. One notable difference lies in the operational model. Digital banks are designed to function without the need for physical branch offices, allowing them to serve customers across Indonesia through electronic platforms. This operational model offers broader service reach and efficiency, making banking more accessible regardless of location. In contrast, conventional banks depend heavily on branch offices to support their daily operations and expand their service coverage. These physical branches play a crucial role in providing face-to-face services and maintaining customer trust, especially in areas where digital literacy may still be limited (Tasman & Ulfanora, 2023).

Digital banks offer a more advanced and seamless transaction experience compared to traditional mobile banking applications. Through digital banking, customers can conduct a wide range of banking activities entirely via dedicated applications. This approach goes beyond the typical features of conventional mobile banking, which primarily replicates ATM functions within a mobile app. While mobile banking in conventional banks allows users to perform basic transactions such as transfers, bill payments, and balance inquiries, digital banks provide a more integrated and user-centric experience. These platforms often include enhanced features such as real-time financial management tools, automated budgeting, personalized financial insights, and customer support directly within the app creating a more dynamic and interactive banking environment (Wijaya et al., 2025).

As an intermediary institution, digital banking plays a vital role in the banking sector and continues to evolve rapidly. Its ability to reach communities across various regions has driven the growing presence of digital banks offering financial services in Indonesia. These digital banks consistently strive to innovate by providing more accessible banking services through the use of technology. One of the key innovations introduced by digital banks in Indonesia is a service known as Account Linkage. This service simplifies customer transactions by utilizing Application Programming Interface (API) Integration, which connects two or more application systems. Through this process, interconnected applications can seamlessly provide access and facilitate the exchange of financial data, enabling smoother and more efficient banking experiences for users (Anderson, 2020). Through the Account Linkage service, customers are able to access data stored in Bank X's application and even carry out banking transactions via links embedded within e-commerce platforms. The presence of the Account Linkage service establishes a new form of connection between banks and third-party platforms, creating a more integrated financial ecosystem. This interconnectedness enables users to perform financial activities more conveniently while also introducing new dynamics in the relationship between banks, customers, and digital service providers (SeaBank, 2024).

Based on research findings, users of digital banking show a considerable level of interest in the Account Linkage service, making it an attractive feature for customers. Although there is currently no specific legislation that directly regulates the legal protection of Account Linkage services, this feature has already been implemented by Digital Bank X in Indonesia.

Its application has proven to provide greater convenience for customers in conducting financial transactions, reinforcing the value and potential of such innovations in the digital banking landscape (Pratiwi et al., 2023).

However, behind the convenience offered by the Account Linkage service, there are inherent risks to customer data security that must be carefully considered. This service involves the disclosure or transfer of customer data between the bank and its e-commerce partners. Such data sharing increases the potential risk of data breaches, particularly through third-party applications or digital bank partners, as several banking services are accessible via these partner platforms. If a data breach occurs within the Account Linkage system due to negligence on the part of the partner or the bank itself, it is essential to determine which party should be held fully responsible for the incident. To ensure a secure Account Linkage service, legal protection and certainty are crucial. Both digital banking institutions and all related parties involved in data exchange must adhere to and implement applicable laws, particularly the Personal Data Protection Law and other relevant regulations. These legal frameworks are necessary to establish clear accountability in the event of a data breach.

Based on the author's literature review, no academic work has been found that discusses this specific topic in depth. However, several related studies have been identified, such as *"Personal Data Protection Law in Digital Banking Governance in Indonesia"* by Wardah Yuspin, Kelik Wardiono, Aditya Nurrahman, and Arief Budiono. This article focuses on regulations for personal data protection in digital banking in Indonesia and compares them with those of other countries. Another relevant work is *"Legal Protection for Digital Bank Customers in Indonesia: Analysis of Data Confidentiality Regulations and Bank Responsibility"* by Sriono, Risdalina, Kusno, Indra Kumalasari M., and Hengki Syahyunan, which discusses the legal protection of customer data confidentiality and general regulations. A further study, *"Legal Protection for Digital Bank Customers in Indonesia with Legal Certainty"* by Kautsar Ismail, Rizky Ramadhan, Raya Arva Rizky Reswara, and Indah Rahmawati Sugita, addresses the legal certainty and protection afforded to customers of digital banks in Indonesia.

This legal writing aims to establish protection and legal certainty for customers, particularly in relation to personal data protection and accountability for data breaches within the Account Linkage service. It emphasizes the need for clear responsibilities among the parties involved, especially government authorities such as the Financial Services Authority (OJK) and Financial Service Providers (Digital Banks) as the providers of banking services. Ensuring strong legal safeguards and coordinated oversight is essential to maintain customer trust and support the secure development of digital banking innovations.

METHOD

This study employs a normative legal research method (juridical normative). In English, this approach is known as *normative legal research*, and in Dutch as *normatief juridisch onderzoek*. Normative legal research is a type of study that places law as a system of norms. These norms include principles, rules, and legal standards derived from statutory regulations, court decisions, agreements, and legal doctrines. This method is used to explore and analyze legal issues, particularly focusing on legal certainty and accountability regarding data breaches in Account Linkage services within digital banking in Indonesia.

Data for this research is collected through library research. Primary data includes statutory regulations, court decisions, and agreements relevant to personal data protection and digital banking services. Secondary data is drawn from legal literature, scholarly articles, journals, official documents, and other supporting materials related to the topic. These sources form the basis for legal interpretation and analysis throughout the study.

The research uses a qualitative analysis technique with a descriptive approach. The analysis involves legal interpretation of relevant laws and regulations, supported by systematic and comparative approaches to assess the coherence and applicability of existing legal norms. This method allows the researcher to examine the adequacy of current legal protections and the responsibilities of stakeholders in the event of data breaches involving Account Linkage services. The findings are expected to provide a comprehensive understanding of the legal protection and accountability framework within Indonesia's digital banking landscape.

RESULTS AND DISCUSSION

Legal Basis for Customer Data Protection in Digital Banking Practices

Data protection is a human right as enshrined in Article 28G of the 1945 Constitution of the Republic of Indonesia, which states: "Every person shall have the right to the protection of their personal self, family, honor, dignity, and property under their control, and shall have the right to security and protection from fear to take or not take action as a human right." The protection of personal data is an integral part of human rights that must be safeguarded through various legal policies in order to create legal certainty (Niffari, 2020).

Within the scope of Digital Banking, the confidentiality of customer data is a crucial aspect, as stipulated in Article 40 Paragraph 1 of (Undang-Undang (UU) Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, 1998), which states: "Banks are obliged to keep confidential information concerning depositors and their deposits." The principle of confidentiality is fundamental and forms part of the obligations between banks and their customers. In fulfilling the protection of personal data, banks are responsible for safeguarding the confidentiality of customer information. The effort to protect personal data cannot be separated from the current legal regulations, which serve as a concrete form of legal certainty, particularly as outlined in Law Number 27 of 2022 concerning Personal Data Protection. This law aims to enhance the effectiveness of personal data protection, ensuring that the processes of protection and accountability in data management are aligned with applicable legal provisions (Puspitasari et al., 2023). (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022) governs the management of data and outlines the responsibilities of all parties involved in the process of providing, controlling, and processing personal data.

In the development of digital banking today, the Account Linkage service has been introduced, in which Bank "X" collaborates with e-commerce partners as beneficiaries of the feature. As an integral part of digital banking, Account Linkage is a service that allows customers to access certain functionalities, such as balance information, biometric data, transaction records, and more. The implementation of Account Linkage is governed by Bank "X" through its responsibility for services and privacy policies regarding customer data. Fundamentally, this is intended as part of an effort to protect personal data and provide legal certainty for customers. However, in the application of service terms and policies imposed by Bank "X" on Account Linkage users, there is a misalignment with the prevailing laws and regulations. Within its banking service terms, Bank "X" includes an Exoneration Clause in the agreement or service contract, particularly for the Account Linkage feature. An Exoneration Clause is defined as "a clause in an agreement in which a party is released from or limits certain liabilities that would normally, under the law, be their responsibility (Manumpil, 2016)."

The inclusion of an exoneration clause in the implementation of the Account Linkage service by Bank "X" represents an attempt to avoid liability for data misuse committed by third parties or other unauthorized entities. Furthermore, the presence of the Account Linkage service necessitates the disclosure or granting of access to partners regarding customers' savings data and other forms of information, which are eventually used within partner-owned services or applications. This practice is perceived to deviate from the fundamental principles

of banking confidentiality regarding customer data. Funds and data collected by banks in the form of deposits and other entrusted information are given by customers based on trust in the banking institution. Therefore, banks must bear full responsibility for maintaining the security and confidentiality of all customer financial information and personal data (Yetno, 2024).

Exoneration Clause in Banking Service Terms and Privacy Policy

In the privacy policy and terms of service of Bank X concerning the Account Linkage feature, there is a clause stating that customers are responsible for the use and protection of information related to their account number, account balance, transaction history, digital bank-registered phone number, one-time password (OTP), partner account, and password including in the event of misuse of such information. Customers bear full responsibility for any consequences resulting from the misuse of their partner account and its associated password. These clauses can be classified as exoneration clauses, which are intended to release the bank from obligations and liabilities concerning any losses related to data protection, customer information, and data breaches during the use of services, including the Account Linkage feature.

Certainly, in an effort to provide legal certainty for customers—particularly in the protection of customer data—digital banking institutions are not limited to regulating data protection efforts solely through their banking service terms. Privacy policies also play a crucial role, as they govern the accountability of digital banks over the products or services provided to customers.

Referring to the privacy policy of Bank X, as a digital bank operating under the sovereignty of Indonesian law, Bank X bears responsibility for its privacy policy in accordance with prevailing regulations, particularly Law Number 27 of 2022 concerning Personal Data Protection. Recognition of this law is clearly stated within Bank X's privacy policy. However, other clauses within the same policy may severely compromise customers' interests, especially regarding disclaimers about the security of third-party websites.

The privacy policy includes a disclaimer clause concerning the security of third-party websites. Through this clause, Bank X disclaims any responsibility for the security of personal data or information provided by customers to third parties. Furthermore, the policy states that Bank X may choose third parties that allow account linkages or services via external websites, partners, or third parties, all of which have their own privacy policies and security settings. This provision applies without exception to affiliated partners, and Bank X claims to have no control over these linked websites. The presence of such clauses introduces legal uncertainty and undermines the accountability of the bank as the service provider.

Moreover, there are regulations that prohibit the inclusion of exoneration clauses in standard agreements or terms of service (including privacy policies) set by the bank. This is stipulated in (Undang-Undang (UU) Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, 1999), Article 18 Paragraph 1(a), which prohibits business actors from including standard clauses that transfer their responsibilities to consumers in any documents or agreements (Ticoh, 2024). In the financial services sector, this is further reinforced by the Financial Services Authority Regulation (POJK) Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, Article 22, which prohibits the inclusion of exoneration clauses that increase the rights or reduce the obligations of financial service providers (PUJK) or consumers, and that shift the responsibility or obligations of PUJK onto consumers.

Therefore, the inclusion of an exoneration clause in an agreement or standard clause imposed by a bank, which aims to transfer responsibility to consumers in a manner that may result in consumer loss, shall be null and void by operation of law. Consequently, if a data breach occurs within the Account Linkage service, the bank, as the service provider, holds responsibility for such a breach. This is in accordance with the applicable regulations,

particularly Article 35 of (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022), which stipulates that "Personal Data Controllers are obligated to protect and ensure the security of the Personal Data they process." This article affirms the responsibility and duty of the banking institution, both as a provider of financial services and as a data controller (Valentina, 2024). Furthermore, Article 36 of the same law also outlines the "obligation of Personal Data Controllers to maintain the confidentiality of personal data." Referring to the applicable Personal Data Protection regulations, the responsibility for safeguarding customer data lies with the Data Controller in this case, the bank. Article 47 of (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022) further mandates that "A personal data controller shall be responsible for the processing of personal data and must demonstrate accountability in fulfilling the obligations to implement the principles of personal data protection."

Referring to Article 40 of (Undang-Undang (UU) Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, 1998), it regulates the obligation of banks to maintain the confidentiality of customer information, particularly concerning customer identity and their deposits. This provision also applies to affiliated parties. The obligation to preserve customer confidentiality is intended to ensure protection for depositors (Rossana, 2016). Therefore, based on the prevailing regulations, any liability arising from a data breach within the Account Linkage service falls under the responsibility of the bank or the Financial Services Provider (PUJK), as the service provider and personal data controller.

The Supervisory Role of the Financial Services Authority (OJK) in the Event of Data Breaches in Account Linkage Services

In the implementation of oversight related to Account Linkage services in Indonesia, the Financial Services Authority (OJK) plays a direct supervisory role in banking practices, particularly concerning consumer and public protection (Syahranni et al., 2023). As of now, Account Linkage services do not yet have specific regulations governing their implementation in alignment with existing laws. Given the interconnection of customer data with banking partner applications, there is a significant possibility that such data may be accessed by third parties. Therefore, OJK must ensure that its supervisory mechanisms function effectively as preventive measures against potential security risks and technological challenges.

The Financial Services Authority (OJK) plays a crucial supervisory role in the banking sector, as mandated under Article 34 of (Undang-Undang (UU) Nomor 3 Tahun 2004 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 23 Tahun 1999 Tentang Bank Indonesia, n.d.). One of its key functions is to ensure that financial services, including Account Linkage, are delivered in a manner that prioritizes consumer safety and accountability. This oversight responsibility is outlined in (Undang-Undang (UU) Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan, 2011)concerning the Financial Services Authority, particularly in Article 28, which authorizes OJK to take preventive actions to protect consumers and the public. These actions include providing education and information about financial services and products, ordering financial service institutions to cease potentially harmful activities, and implementing other necessary measures in accordance with financial sector regulations (Syahranni et al., 2023).

Based on Article 28, OJK has the authority to oversee and protect consumers in all aspects of financial services, including digital banking services like Account Linkage. As part of its supervisory efforts, OJK may conduct reviews and evaluations of these services to prevent risks and ensure accountability in protecting customers. These responsibilities are further elaborated in the (Undang-Undang (UU) Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan, 2011) concerning Consumer and Public Protection in the Financial Services Sector.

This regulation serves as a legal foundation to monitor the conduct of Financial Services Business Actors (PUJK) in delivering financial products and services. Article 3 of (Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan, 2023) mandates that PUJK must adopt the principles of consumer protection in their business operations. These principles include adequate education, transparency and openness in product and service information, fair treatment and responsible business conduct, protection of consumer assets, privacy and data, effective complaint handling and dispute resolution, enforcement of compliance, and healthy competition.

Under these provisions, banks as service providers are obligated to implement these principles, particularly those concerning the protection of customer data and privacy as outlined in Article 3 paragraph (2) letter d. Any PUJK that fails to uphold these principles may be subject to administrative sanctions as stipulated in Article 3 paragraph (3), which include written warnings, restrictions or freezing of products and services, removal of executives, administrative fines, and revocation of licenses. To further ensure protection and legal certainty for consumers, Article 4 paragraph (1) of (Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan, 2023) requires PUJKs to act in good faith when conducting business activities or offering financial products and services. In line with this, banks must take full responsibility for upholding customer rights and are required to safeguard customer interests, especially in relation to the delivery and use of Account Linkage services.

CONCLUSION

The current implementation of Account Linkage services in digital banking has not yet fully ensured the protection of customers' personal data, particularly due to the presence of exoneration clauses that potentially shift responsibility from the bank to the customer. This condition reflects a gap in existing legal policies, highlighting the urgent need for a review and the formulation of specific regulations governing the practice and protection within Account Linkage services. The Financial Services Authority (OJK), as the supervisory body, plays a crucial role in enforcing strict oversight and establishing rules that support consumer protection. Banks, as digital service providers, are obligated to be accountable for the security, management, and safeguarding of customers' personal data by adhering to the principles of prudence and good faith. The responsibility of banks to maintain the confidentiality of customer data is not only a legal obligation but also a fundamental principle in banking operations that must be upheld to maintain public trust.

REFERENCE

Anderson, C. (2020). Not the same: Open banking, open APIs and banking as a service. *BBVA. Accessed May*, *4*, 2022.

Manumpil, J. S. (2016). Klausula Eksonerasi Dalam Hukum Perlindungan Konsumen Di Indonesia. *Lex Privatum*, *4*(3). https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/11547

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, *7*(1), 105–119.

Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan, Pub. L. No. 22 (2023).

Pratiwi, A., Wahyuningsih, L., & Az, S. A. (2023). Sosialisasi Pelayanan Dan Produk Di Bank Muamalat Kcp Banyuwangi. *Jurnal Pengabdian Masyarakat Dan Lingkungan (JPML)*, *2*(1), Article 1. https://doi.org/10.30587/jpml.v2i1.5686

Purwanto, A. (2022, July 24). Bank Digital: Prospek dan Tantangan di Indonesia. *Kompaspedia*. https://kompaspedia.kompas.id/baca/paparan-topik/bank-digital-prospek-dan-tantangan-di-indonesia

Puspitasari, D., Izzatusholekha, I., Haniandaresta, S. K., & Afif, D. (2023). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk. *Journal of Administrative and Social Science*, *4*(2), 195–205.

Rossana, G. (2016). Penafsiran Pasal 40 Undang-Undang Nomor 10 Tahun 1998 Mengenai Kerahasiaan Bank. *Lambung Mangkurat Law Journal*, *1*(2), 119–128. https://doi.org/10.32801/abc.v1i2.19

SeaBank. (2024). *Syarat & Ketentuan*. https://www.seabank.co.id/info/syarat-layanan-perbankan

Simatupang, S., Sinaga, O. S., Manurung, S., Ambarita, M. H., & Mokodongan, E. N. (2024). Bank Digital Dan Kepercayaan Konsumen. *Jurnal Ilmiah Satyagraha*, *7*(2), Article 2. https://doi.org/10.47532/jis.v7i2.1090

Syahranni, A., Azdy, D., Putri, S., & Sudirman, D. C. (2023). Analisis Yuridis Terkait Penerapan Euthanasia Yang Dilakukan di Indonesia Berdasarkan Perspektif Hukum Pidana. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *1*(3), 100–113. https://doi.org/10.59246/aladalah.v1i3.336

Tasman, T., & Ulfanora, U. (2023). Perlindungan Hukum Terhadap Nasabah Bank Digital. *UNES Law Review*, *6*(1), Article 1. https://doi.org/10.31933/unesrev.v6i1.962

Ticoh, S. W. (2024). Penerapan Eksonerasi Dalam Suatu Perjanjian Kontrak Proyek Pembuatan Jalan Pemerintah. *LEX PRIVATUM*, *13*(4). https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/56590

Undang-Undang (UU) Nomor 3 Tahun 2004 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 23 Tahun 1999 Tentang Bank Indonesia, Pub. L. No. 3.

Undang-Undang (UU) Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Pub. L. No. 8 (1999).

Undang-Undang (UU) Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, Pub. L. No. 10 (1998).

Undang-Undang (UU) Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan, Pub. L. No. 21 (2011).

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. 27 (2022).

Valentina, D. D. (2024). *Keabsahan Penggunaan Klausul Eksonerasi Dalam Transaksi E-Commerce Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen*. https://digilib.uns.ac.id/dokumen/112205/Keabsahan-Penggunaan-Klausul-Eksonerasi-Dalam-Transaksi-E-Commerce-Berdasarkan-Undang-Undang-Nomor-8-Tahun-1999-Tentang-Perlindungan-Konsumen

Wijaya, A., Hartono, C., & Arwanto, B. (2025). Perlindungan Hukum Nasabah Bank Digital Syariah di Indonesia yang Berkepastian Hukum. *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)*, *5*(3). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=27472000&AN=183769016&h=b80%2BfmG7cbVyWrkZLa2BKgSHuIs7f%2BWRF%2BNG3ViWvsjVUvzIrijovx4Q4UkcTWZ%2BbP%2FzFImCUzZHrLxtU7l0oQ%3D%3D&crl=c

Yetno, A. (2024). Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia. *MORALITY: Jurnal Ilmu Hukum*, *10*(1), 67–76.