EAS Journal of Humanities and Cultural Studies
Abbreviated Key Title: EAS J Humanit Cult Stud
ISSN: 2663-0958 (Print) & ISSN: 2663-6743 (Online)
Published By East African Scholars Publisher, Kenya

Volume-6 | Issue-3 | Jul-Aug-2024 | DOI: https://doi.org/10.36349/easjhcs.2024.v06i03.009

OPEN ACCESS

Original Research Article

Banking Customer Data Security Protection in the Era of Financial Technology in Indonesia

Nadhira Candra[1*], Dewi Astuty Mochtar[1], Kadek Wiwik Indrayanti[1]

[1]University of Merdeka Malang, Jalan Terusan Dieng. 62-64 Klojen, Pisang Candi, Sukun, Malang City, East Java 65146, Indonesia

Article History
Received: 16.07.2024
Accepted: 21.08.2024
Published: 23.08.2024

Journal homepage:
https://www.easpublisher.com

Quick Response Code

Abstract: This research aims to identify and analyze legal protection for the security of banking customer data in the era of financial technology in Indonesia and banking policies and programs for maintaining the security of customer data based on related regulations. The research method used is normative juridical. The results of the research state that the protection of the security of customers' data related to financial technology has been regulated in several statutory regulations starting from Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning Legal Protection of Personal Data in Electronic Systems, Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology, and Financial Services Authority Regulation POJK No. 1/POJK 07/2013 concerning Consumer Protection in the Financial Services Sector and ITE Law No. 11 of the Year 2008 concerning Information and Electronic Transactions. Meanwhile, banks in Indonesia have policies and programs.

Keywords: Banking, Data Security, Fintech, Legal Protection.

1. INTRODUCTION

Based on the We Are Social report, in January 2024, there will be 185 million internet users in Indonesia, equivalent to 66.5% of the total national population of 278.7 million people. At the beginning of this year, internet users in Indonesia were recorded to have increased by around 1.5 million people, or an increase of 0.8% compared to January 2023 (https://databoks.katadata.co.id/datapublish/2024/02/27/ada-185-juta -internet-users-in-Indonesia-in-January-2024), furthermore, according to the 2021 edition of the State of Finance App Marketing report, released by Appsflyer. Among 15 other countries, Indonesia ranks third in this regard, indicating that Indonesians depend on financial applications to meet their various financial needs. Behind the convenience offered by financial applications, many risks are also involved. Irresponsible parties can use security gaps to collect personal information such as account numbers, balances, credit and debit card information, and transaction records.

The definition of Fintech is juridically found in the Bank Indonesia Fintech Regulations (PBI). Based on Article 1 paragraph (1) PBI No. 12/19/PBI/2017 Regarding the Implementation of Financial Technology (from now on referred to as PBI Fintech): "Financial Technology is the use of technology in the financial system that produces new products, services, technology, and business models and can have an impact on monetary stability, system stability financial, and efficiency, smoothness, security and reliability of the payment system. "More efficient financial services using technology and software can easily be achieved with Fintech. Financial transactions through Fintech include payments, investments, borrowing money, transfers, financial plans, and financial product comparisons. The concept of financial technology adapts technological developments combined with the financial sector in banking financial institutions to facilitate a more practical, safe, and modern financial transaction process. According to data from the Indonesian Fintech Association, in mid-2017, 90 Fintech startup companies were members, and the number increased to 103 Fintech startup companies in the third quarter of 2017.

In Indonesia, several types of Fintech have been developed, including online payment, peer-to-peer, insure tech, aggregator, and crowdfunding. Each type of Fintech has potential risks according to its business processes. In general, the risks that may arise from Fintech companies in Indonesia are Fraud risk, Data security risk, and Market uncertainty risk.

***Corresponding Author:** Nadhira Candra
University of Merdeka Malang, Jalan Terusan Dieng. 62-64 Klojen, Pisang Candi, Sukun, Malang City, East Java 65146, Indonesia

In 2020-2024, there were 192,000 reports regarding accounts that indicated online fraud and other types of reports received by Ministry of Communication and Information related to online prostitution, extortion, fictitious online investments, and other crimes. The account report indicated that Ministry of Communication and Information received criminal via the official website CekRekening.id. Sites belonging to traditional banks have also begun to strengthen their presence on digital platforms.

He was starting with the case of X (52), a vehicle accessory entrepreneur. His savings in his bank account, which reached IDR 1.4 billion, disappeared because he clicked on the wedding invitation via WhatsApp (WA). The savings of a priority customer of one of these state-owned banks disappeared overnight. Funds in account X moved without prior confirmation as a customer or account owner. Of the total savings of IDR 1.4 billion, it disappeared in an instant, and only 2 million remained in the account. Based on the description above, this article examines legal protection for the security of banking customer data in the era of financial technology and banking policies and programs in maintaining the security of customers/data.

2. METHODOLOGY

The type of research used is normative legal research. Normative legal research is a process for determining legal rules, principles, and doctrines based on a legal issue. The statutory approach and conceptual approach are used.

3. RESEARCH RESULT

3.1 Legal Protection of Customer Data in Indonesia

The Indonesian government, through Bank Indonesia (BI) and the Financial Services Authority (OJK) as the bodies with authority to regulate Fintech according to its category, have issued technical regulations in regulations related to Fintech, including Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) regulates that individuals, including those who carry out business or e-commerce activities at home, can be categorized as personal data controllers (Agustini *et al*., 2024). So, he is legally responsible for the processing of personal data that he holds and fulfills the provisions in the PDP Law, stipulating that individuals, including those who carry out business or e-commerce activities at home, can be categorized as personal data controllers. So he is legally responsible for processing personal data that he holds and fulfills the provisions of the PDP Law (Ariska *et al.*, 2024). Meanwhile, suppose a bank employee or other affiliated party provides the customer's confidential information. In that case, he will be charged under Article 14 number 51 of the P2SK Law, which amends Article 47 paragraph (2) of Law 10/1998, which states that members of the board of commissioners or equivalent, members of the board of directors or equivalently, bank employees or other affiliated parties who deliberately provide information (which must be kept confidential) according to Article 40, are threatened with imprisonment for a minimum of 2 years and a maximum of 4 years and a fine of at least IDR 4 billion and a maximum of IDR 8 billion (Djati & Purwaningsih, 2024).

Furthermore, PBI No. 19/12/PBI/2017 Concerning the Implementation of Financial Technology (from now on referred to as PBI Fintech), PBI No. 18/40/PBI/2016 concerning Implementation of Payment Transaction Processing, PBI No. 11/12/PBI/2009 Concerning Electronic Money which has been amended in PBI No. 16/8/PBI/2014. The next stage is that Fintech expands to include all technology-based financial services, no longer a private non-bank institution that only does business in this area of technology (Fathoni *et al*., 2024).

Law Number 27 of 2022 concerns the Protection of Personal Data Security, while other statutory regulations support the existing legal umbrella (Hendarto, 2024). Meanwhile, suppose a bank employee or other affiliated party provides the customer's confidential information. In that case, he will be charged under Article 14 number 51 of the P2SK Law, which amends Article 47 paragraph (2) of Law 10/1998 which states that members of the board of commissioners or equivalent, members of the board of directors or equivalently, bank employees or other affiliated parties who deliberately provide information (which must be kept confidential) according to Article 40, are threatened with imprisonment for a minimum of 2 years and a maximum of 4 years and a fine of at least IDR 4 billion and a maximum of IDR 8 billion (Indahyani *et al*., 2024).

Then, legal protection for bank customers is also regulated in Law Number 21 of 2011 concerning the Financial Services Authority. However, it is not a legal protection law. However, consumer protection is one of the objectives of the Financial Services Authority Law. Consumer protection in Law Number 21 of 2011 concerning the Financial Services Authority includes more complex and complete consumer protection. With increasingly wider coverage, the scope of tasks, authority, and responsibility for consumer protection by the Financial Services Authority also becomes wider in the financial services sector. In Article 4, letter (c) of Law Number 21 of 2011 concerning the Financial Services Authority, the aim of establishing the OJK institution is so that all activities in the financial services sector can protect the interests of consumers and the public. Customers as consumers are obliged to receive legal protection for the use of service products offered by the Bank. Legal protection is an effort to maintain the trust of the wider community, especially customers (Madin, 2024).

This incident has caused users to lose large amounts of funds due to hacking attempts and data theft

by irresponsible parties. Even though Law Number 27 of 2022 concerning Information and Electronic Transactions (UU ITE) has been promulgated as a legal umbrella to regulate information security and electronic transactions, the data breach incident at DANA indicates that there are areas for improvement in the implementation of the IT Protection of personal data should be the government's responsibility, because personal data is part of the human rights of every citizen. The presence of the ITE Law is the government's effort to guarantee security and protect the interests and rights of electronic service users, especially regarding protecting personal data and personal information (Martinelli *et al.*, 2024). The ITE Law regulates the limitations, obligations, and responsibilities of parties involved in administering electronic systems, such as service providers, data managers, and end users. In addition, the ITE Law regulates criminal acts related to violations of information security and electronic transactions and sanctions that can be imposed on cyber criminals. It is in his control. The main focus on efforts to protect personal data in the Fintech industry can also be done by: 1) Encrypting data relating to consumers, Fintech service players must do this; 2) The security of consumer data is something that Fintech service players must maintain; 3) Data access management is mandatory for Fintech service providers; 4) From the consumer side, there needs to be a consumer right to request and receive an explanation from Fintech service providers regarding the use of consumer data and information that has been given to them (Munah & Deni, 2024).

Considering Bank Indonesia Regulation Number 19/12/PBI/20178 concerning the Implementation of Financial Technology, it was explained that this regulation was made by considering the community's needs regarding innovation in financial technology services. For the sake of improving and developing financial technology, it has been regulated in Bank Indonesia regulation Number 19/12/17, specifically in Article 11 paragraph (1) that every financial technology operator must first be tested through the Regulatory Sandbox organized by Bank Indonesia (Nawakshara & Purwaningsih, 2024). The Regulatory Sandbox aims to prevent various risks inherent in Fintech innovation when products are marketed, such as customer confidentiality, data theft, cyber-attacks, and various other risks. Then, some sanctions must be accepted regarding violations committed by financial technology providers. Sanctions will be received if financial technology providers do not register and have violated various provisions specified in this regulation.

The regulations regarding sanctions can be seen in Article 20 paragraph (1), Article 20 paragraph (2), and Article 20 paragraph (3) Bank Indonesia Regulation Number 19/12/17 8. In these articles, various sanctions have been regulated, and all of them are included in administrative sanctions. Regarding personal data protection, one of the provisions is regulated in Article 8 paragraph (1), which contains obligations as a registered financial technology operator. One of the obligations is to maintain the confidentiality of consumer data and information, including transaction data and information (Nawakshara & Purwaningsih, 2024). OJK, as an institution that has the authority to supervise business activities in the financial services sector, is determined in Article 4 Letter c of Law no. 21 of 2011 concerning the Financial Services Authority, which states that one of the objectives of establishing the OJK is to be able to protect the interests of consumers and the public in the financial services sector (Pratama & Octaris, 2024). As users of financial services, Fintech consumers have the right to obtain protection for their data from Fintech companies that provide financial services to them. Therefore, OJK, through Financial Services Authority Circular Letter No. 14/SEOJK.07/201411 concerning Confidentiality and Security of Consumer Data and Personal Information, personal data that must be protected in Fintech business in Indonesia are Individual and corporate data (Rianda, 2024). This is made clear in the Financial Services Authority Circular Letter No.18/SEOJK.02/201712.

One form of legal protection is by creating legal regulations that provide certain conditions that must be fulfilled by fintech companies that want to open their businesses in Indonesia. Another form of legal protection is by requiring fintech companies to collaborate with financial institutions such as banks to provide more legal protection and certainty for customers or consumers (Rivano *et al*., 2024). Collaborating with banks and transferring innovation to the Bank is an obligation. Collaboration between fintech companies and banks is also necessary to save banks from losing customers due to switching to easier and more innovative Fintech. Several policies that OJK can implement.

3.1.1 Supervision and regulation that focuses on Fintech that has developed and is used in Indonesia

To accelerate consumer protection efforts related to FinTech products in Indonesia, the OJK, as a regulator, needs to determine the focus on FinTech that has and will develop in Indonesia. This focus includes Fintech lending, Fintech payments, and Fintech supporting (Fintech scoring, Fintech information site, Fintech financial management, and Fintech big data analytics). As for Robo-Advisors, Blockchain, and Bitcoin, although these are important things, they are not yet urgent things to do at this time because the literacy level of Indonesian society does not yet support the development of these types of Fintech (Sudirman *et al*., 2024).

After determining the focus area, the OJK can immediately map the relevant regulations in Indonesia. Unlike Singapore, Australia, or England, which apply a legal system that is Common Law, Indonesia applies a legal system that is Continental European (Civil Law), where everything must be stated and recorded clearly in Law. If there is no legal regulation for a type of Fintech

development in Indonesia, then if a problem occurs, there is no legal basis to resolve it. This is also related to consumer protection. By the OJK's authority in the financial services sector, Fintech from PUJK related to the financial services sector can be regulated based on the OJK Law and the Laws in each financial services sector. Existing laws in the banking sector can regulate Fintech related to the banking sector and Fintech related to the capital markets sector and non-bank financial institutions (for example, insurance, financing, pawnshops). Meanwhile, Fintech related to payment services can be regulated using Bank Indonesia regulations (Rivano *et al*., 2024).

OJK should develop standards or guidelines related to aspects of consumer protection in Fintech products/services that fall within the scope of its authority, complementing other guidelines related to service operations. The three OJK supervisory sectors (Banking, NBFI, and Capital Markets) can later use these guidelines to supervise. Increased coordination with related stakeholders. OJK should coordinate and collaborate with other Fintech stakeholders, to complement Fintech regulations, avoiding duplication of overlapping regulations (duplicative regulations), and b) Mitigating potential risks and challenges in achieving a balance between the development of the national financial system, Fintech developments, and consumer protection aspects.

This coordination was carried out with the Coordinating Ministry for Economic Affairs, Bank Indonesia, Ministry of Trade, Ministry of Finance, Ministry of Communication and Information, Ministry of Law and Human Rights, associations in the financial services sector, Fintech associations and practitioners, and academics. With good coordination, it is hoped that Fintech regulations can be realized nationally and well coordinated.

Apart from that, Regtech (Regulatory Technology) companies currently can support Fintech players to ensure they comply with related regulations. OJK needs to support the use of Regtech in Fintech service providers' business activities. The benefit of using the Regtech feature is that it can increase compliance with existing regulations and maximize the risk management function of service providers. Apart from that, Regtech's features can minimize violations of the provisions that the OJK has prepared. With the automation feature of reports and documents related to transactions between Fintech players, Regtech can detect and analyze if there are suspicious transactions or violations of existing regulations. Suppose OJK can encourage the use of Regtech. In that case, OJK can support the establishment of Fintech services that comply with existing regulations so that consumers and the public can enjoy safe use of services and do not need to be afraid of feeling disadvantaged. OJK can collaborate with Supervisory Technology (Suptech) service providers to support digital supervision. Some Suptechs have key features such as data reporting automation, data validity analysis, and report standardization. These features can make it easier for supervisors to analyze data provided by financial service institutions and other Fintech service providers. Besides that, Suptech can also speed up the monitoring process, which usually requires quite a long duration because supervision is carried out using manual analysis methods from very large amounts of data. By automating the delivery of accurate reports and collecting valid data, Fintech supervision efforts can be more optimal, effective, and efficient.

3.1.2 Increased Fintech legitimacy

Regarding this effort, there are three things that OJK can implement to increase the legitimacy of Fintech in Indonesia. a) OJK or related regulators can impose a Trustmark (which can be in the form of a logo, image, or badge) on all sites and applications of Fintech players that have been registered and supervised. This Trustmark will also show that the Fintech system has been audited either by a regulator or another appointed party. b) Implement a digital signature certificate which will authenticate consumer identity electronically using a signature. c) Implement biometric verification that can identify one or more unique biological characteristics of consumers. This unique identification can include fingerprints, palm geometry, retinal patterns, and sound waves. It is believed that the OJK or other regulators can use the three methods above to increase public and consumer confidence in Fintech products/services because they can mitigate potential risks such as the risk of fraud, the risk of forgery or identity theft, and the risk of hackers. Trustmarks have been implemented to legitimize the security of e-commerce businesses, and several trustmark providers exist today.

3.2 Policies and Programs in several Banks in Indonesia

The Financial Services Authority Regulation regulates banking policies for handling customer data security cases no. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector as well as Article 40 (1) of Law no. 10 of 199849 concerning Banking concerning the obligation of banks to keep confidential information regarding depositors and their deposits, as an institution with authority to handle cases in the banking sector.

3.2.1 Private Bank

Bank Central Asia (BCA) uses various methods to keep your data safe and protected, such as encryption technology and other forms of security. In addition, BCA also requires BCA staff and other parties who collaborate with BCA to comply with all applicable provisions regarding the protection of Personal Data and implement security measures in processing Personal Data. BCA may change, supplement, and replace this Privacy Policy from time to time to ensure that this Privacy Policy is in

line with the procedures and practices carried out by BCA in processing Personal Data. BCA will provide the latest Privacy Policy via the BCA website at www.bca.co.id.

3.2.2 Conventional Banks

Bank Negara Indonesia (BNI). BNI has a policy called Good Corporate Governance, abbreviated as GCG, which is a bank governance that applies the principles of openness, accountability, responsibility, independence, and fairness. GCG principles must be implemented in all activities of the Board of Commissioners, Directors, all BNI employees, and all parties who work in the interests of BNI. The Board of Commissioners supervises and ensures the implementation of GCG principles in every BNI business activity at all levels of the BNI organization. In its implementation, GCG must guarantee BNI's ability to create superior performance and add economic value for Shareholders and Stakeholders while ensuring that BNI operates by complying with legal discipline, business ethics, and BNI's code of ethics.

Regarding the Data Security Policy, do not reveal your banking transaction data and information to any party, including BNI officers, because BNI never asks for information such as OTP, User ID, MPIN, Transaction Password, BNI Mobile Banking, SMS Banking PIN, Debit Card PIN and Credit Card, CVV or CVC Card (last three numbers on the back of your physical card). Furthermore, the BNI Mobile Banking Privacy Policy can be described as follows: BNI Customer Data, whether in the form of personal data or funds held in the Bank, is a Bank Secret protected by the Bank and refers to the provisions of the applicable Law. BNI uses Secure Socket Layer (SSL) encryption technology in the BNI Mobile Banking application to ensure confidentiality and security, which will protect communications between Customer devices and BNI servers. Security at BNI Mobile Banking uses the time-out session method for 5 (five) minutes.

3.3 Banking Policy Efforts

The cause of this customer data leak problem can be through external or internal sources, such as human error or accidental HR (employees) who accidentally send sensitive information online. Another cause of this data leak is malware or intruders entering via email, internet downloads, or infected programs. Customer data security is an important thing that is of concern to the banking industry in order to provide customer service and trust. This data security protection focuses on procedures and implementation supported by HR integrity. The following are several efforts and ways the banking industry ensures the security of customer data, namely by using encryption to maintain the security of customer data when it is sent or stored. Encryption is the process of converting data into code that cannot be read by people who do not have the encryption key; it uses a multi-factor authentication system to ensure only authorized people can access customer data. For example, using a combination of secret code, token card, and fingerprint to verify user identity; Maintaining the physical security of customer data by storing the data on well-protected servers and using strict security procedures in data storage centers; Conducting regular security audits to ensure the security system is still effective and address any possible security weaknesses; Providing data security training to banking employees so that they know the importance of customer data security and how to maintain the security of this data; Sign confidentiality agreements with employees, vendors and partners to ensure that customer data will not be disclosed to unauthorized parties.

The policy issued by banking is to create a customer data protection team. This profession is responsible for managing and protecting the data of customers or customers of a company or organization. The main task of a customer data protector is to ensure that customer data is properly protected from unauthorized access and data leaks. To perform this task, a customer data protector may have to work closely with security teams, IT technicians, and other professionals to develop and implement effective data security policies. In addition, the customer data protection profession must monitor data security activities continuously and address any security weaknesses

A customer data protection professional may occupy several work positions, including Data Protection Officer (DPO), Chief Privacy Officer (CPO), or Information Security Manager. Some skills needed for the Customer Data Protection profession are analytical, communication, technical, accuracy, problem-solving, adaptability, and teamwork. This profession related to customer data protection is needed in the current and future technological era. Apart from taking formal education, you can also learn about Customer Data Protection by participating in the Future Career Class Future Skills program related to the Customer Data Protection profession to increase your skills and expertise in this field.

4. CONCLUSIONS

Based on the description above, it can be concluded as follows: Regarding legal protection of personal data, banking customers in Indonesia have received legal protection. Several statutory regulations regulate this, namely Law No. 11 of 2008 concerning Information and Electronic Transactions, Civil Code (Staatsblad of 1847 Number 23), Law Number 8 of 1999 concerning Consumer Protection (State Gazette of the Republic of Indonesia of 1999 Number 42, Law No. 11 of 2008 concerning ITE and the Personal Data Protection Law. Apart from that, there are several regulations such as Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology Based Loan and Borrowing Services (State Gazette of the Republic of Indonesia of 2016 Number 324),

Government Regulation No. 2019 concerning Implementation (State Gazette of the Republic of Indonesia 2016), Financial Services Authority Regulation Number: 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector (State Gazette of the Republic of Indonesia 2018 Number 135, Supplement to State Gazette of the Republic of Indonesia Number 6238), Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Financial Technology (State Gazette of the Republic of Indonesia of 2017 Number 245), Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2012 Number 189).

The policies and programs implemented by private and conventional banks to maintain the security of customer data already exist but vary. Generally, it includes several strategic steps. Banks must continue investing in the latest security technologies, such as encryption, firewalls, and intrusion detection systems. Many banks work with technology companies and cybersecurity service providers to improve customer data protection. This collaboration includes security audits, developing security solutions, and sharing information on the latest cyber threats. Banks are also expected to hold educational programs and awareness campaigns regarding data security for customers and employees. This includes seminars, workshops, and educational materials that explain. Meanwhile, advice can be given on the importance of every Bank having an internal policy covering data handling procedures, employee responsibilities, and actions that must be taken in data breaches. In addition, regular audits and evaluations of data security policies and practices should be carried out.

REFERENCES

- Agustini, R. P., Putri, A. A., Wibowo, D. F., Husna, L. M., & Wandita, C. Y. (2024). Tinjauan Yuridis Akibat Hukum Terhadap Wanprestasi Dalam Perjanjian Jual Beli. *Action Research Literate*, *8*(7). https://doi.org/10.46799/arl.v8i7.458
- Ariska, A., Bahri, E. S., & Sari, S. F. (2024). Merespon Fenomena Berita Perbankan Melalui Artikel: Studi Kasus Asuransi di Indonesia dan Peraturan yang Mengaturnya. *Deleted Journal*, *1*(10), 367–370. https://doi.org/10.55324/jgi.v1i10.103
- Djati, K. N., & Purwaningsih, S. B. (2024). Akibat Hukum dari Tindakan Menyimpang dalam Perjanjian Pembiayaan Modal Usaha dengan Pelaku UMKM. *Deleted Journal*, *1*(3), 13. https://doi.org/10.47134/jcl.v1i3.3062
- Fathoni, M. H., Pieris, J., & Widiarty, W. S. (2024). Analisis Hukum Potensi Akibat Wanprestasi Perjanjian Pemborongan Pekerjaan Pengadaan dan Pemasangan Hospital Elevator di PT. Louserindo Megah Permai. *Action Research Literate*, *8*(7). https://doi.org/10.46799/arl.v8i7.461
- Hendarto, I. S. (2024). Implikasi Pengaruh Minimnya Pengaturan Perlindungan Privasi Data Pribadi Nasabah Pada Perbankan Digital. *Journal Justiciabelen (JJ)*, *4*(02), 129. https://doi.org/10.35194/jj.v4i02.4440
- Indahyani, W. S., Leniwati, D., & Wicaksono, A. P. N. (2024). Financial Performance, Maqashid Syariah dan Corporate Reputation: Moderasi Islamic Corporate Social Responsibility (ICSR). *EL MUHASABA Jurnal Akuntansi (e-Journal)*, *15*(2), 102–118. https://doi.org/10.18860/em.v15i2.23924
- Madin, M. M. (2024). Penggunaan Metode Fuzzy Mamdani Dalam Evaluasi Kepuasan Pelanggan: Studi Kasus Pada Layanan Perbankan Di Bank BRI. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.4775
- Martinelli, I., Sugiawan, F. A., & Zulianty, R. (2024). Kepastian Hukum Kontrak Elektronik Dalam Pinjaman Online Berdasarkan Hukum Perikatan. *JAMPARING Jurnal Akuntansi Manajemen Pariwisata Dan Pembelajaran Konseling*, *2*(2), 537–543. https://doi.org/10.57235/jamparing.v2i2.2922
- Munah, F., & Deni, F. (2024). Perlindungan Hukum Istri Dalam Kepailitan Suami. *Binamulia Hukum*, *13*(1), 277–288. https://doi.org/10.37893/jbh.v13i1.834
- Nawakshara, M. V., & Purwaningsih, S. B. (2024). Keabsahan Kontrak Verbal di Indonesia di Bawah Undang-Undang Ketenagakerjaan. *Deleted Journal*, *1*(3), 15. https://doi.org/10.47134/jcl.v1i3.3079
- Pratama, B. P., & Octaris, H. (2024). Perlindungan Hukum Terhadap Pelaku Usaha atas Tindak Pidana Penggelapan Jaminan Fidusia Pada Tahap Penyidikan. *Deleted Journal*, *1*(3), 234–241. https://doi.org/10.60034/1w1x4g53
- Rianda, C. N. (2024). Prinsip dan Konsep Dasar Bank. 1(2), 100–106. https://doi.org/10.61579/kirana.v1i2.152
- Rivano, M., Khairani, N., & Fatimah, T. (2024a). Akibat Hukum Permberlakuan Perjanjian Kerja Bersama Yang Habis Masa Berlakunya. *Lareh Law Review*, *2*(1), 73–84. https://doi.org/10.25077/llr.2.1.73-84.2024
- Sudirman, L., Disemadi, H. S., & Jerryen, J. (2024). Bentuk Pengaturan Perbankan Digital di Negara Indonesia dan Singapura. *Legal Spirit*, *8*(2), 325–340. https://doi.org/10.31328/ls.v8i2.5438
- Rivano, M., Khairani, N., & Fatimah, T. (2024b). Akibat Hukum Permberlakuan Perjanjian Kerja Bersama Yang Habis Masa Berlakunya. *Lareh Law Review*, *2*(1), 73–84. https://doi.org/10.25077/llr.2.1.73-84.2024

Cite This Article: Nadhira Candra, Dewi Astuty Mochtar, Kadek Wiwik Indrayanti (2024). Banking Customer Data Security Protection in the Era of Financial Technology in Indonesia. *EAS J Humanit Cult Stud, 6*(3), 117-122.