Malikussaleh Social & Political Reviews
Volume 4, Number 1, Mei 2023
ISSN 2746-8100 (online)

DOI : 10.29103/mspr.v%vi%i.11047

Research Original Article

Bank Responsibilities in Guaranting Customer Data at Bank Syariah Indonesia of Lhokseumawe City

Sulaiman[1]
[1]Lecture at Faculty of Law, Universitas Malikussaleh
*Corresponding Author: sulaiman@unimal.ac.id

Abstract
Leakage of customers' personal information data is a recurring problem in Indonesia, which impacts both state-owned and private banks. Leaks occur due to various internal and external factors, creating a significant data misuse risk. To overcome this problem, Law Number 27/2022 concerning the Protection of Personal Data emphasizes the importance of protecting personal information and ensuring proper use. This study investigates the responsibility of Bank Syariah Indonesia in the city of Lhokseumawe in protecting customer data, identifies factors contributing to data breaches, and proposes steps to mitigate the incident. By using empirical normative juridical research methods, this research used a law-based and case-based approach. The findings revealed that Bank Syariah Indonesia Lhokseumawe also experienced data breaches, mainly due to internal and external factors. The actions of bank employees cause internal leaks, while external factors include individuals involved in fraudulent activities to exploit customer data. Urgent action must be taken to effectively address data breaches, including comprehensive security protocols, staff training, and cooperation with relevant authorities. By adhering to these steps, banks can strengthen their data protection practices and effectively mitigate the risks associated with data breaches.

Keywords: Responsibility, Bank Syariah Indonesia, Customer Data

Introduction
Indonesia is a state based on law as referred to in Article 1 paragraph 3 of the 1945 Constitution. Banking traffic is also regulated by legal provisions, such as Law Number 7 of 1992 concerning Banking, as amended by Law Number 10 of 1998 which provides the concept and an understanding of banking principles that use the precautionary principle. Bank is a business entity that collects funds from the public in the form of savings and distributes them to the public in the form of credit and or other forms in order to improve the lives of the general public (Article 1 of Law Number 7 of 1992 as Amended by Law Number: 10 1998, concerning Banking). The introduction of Aceh Qanun Number 11 of 2018 concerning Sharia Finance and Aceh Qanun Number 8 of 2014 concerning Standards of Islamic Shari'a underlines the commitment of each and every monetary institution in the Aceh region to have Shari'a standards.

Banks play a significant part in individuals' lives. Because a variety of economic and commercial transactions necessitate banking institutions, the public as customers and the bank have a synergistic relationship. As a customer, the community provides everything pertaining to their personal identity in this relationship, which must be kept private and may not be published without the customer's consent. In the first paragraph of Article 40 of the banking law, it is emphasized that banks must uphold the confidentiality principle when carrying out their responsibilities. With this principle, parties who have no interest in customer data cannot access it so that the data is safe and does not harm bank customers.. This also applies to the Personal Data Protection Act of 2022, Law No. 27. Law ensures adequate legal protection, but in practice, customer personal data leaks continue to occur in the banking industry.

Literature Review
Juridical Review on Banking.
Etymologically, the word bank comes from the French *banque* and the Italian *banca* means bench. During the Renaissance, transactions were carried out behind a seated money exchange counter. This is very different from other types of work which cannot be done sitting down (Dr Jamin Ginting S.H. M.H., 2017; Sri Wahyuni & Kurniawan, 2022; Wulandari & Ghozali, 2019). Article 1 paragraph 1 and 2 of Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, (1) Banking is everything related to banks, including their institutions, business activities. (2) Bank is a business that collects funds from the public in the form of credit and or other forms in order to improve the standard of living of the people at large.

Law Number 21 of 2008 concerning Shari'a Banking discusses types of business activities that do not violate sharia principles which are businesses that do not contain the following elements (Husen Sobana, 2016) 1. *Riba*, additional income by way of illegitimate (vanity), 2. *Maisir*, transactions that depend on an uncertain condition and are chancy, 3. *Gharar*, i.e. transactions whose object is not clear, are not owned, whereabouts are unknown, or cannot be submitted at the time the transaction is carried out unless otherwise regulated in shari'a, 4. *Haram*, i.e transactions whose objects are prohibited in shari'a, 5. *Zalim*, transactions that cause injustice to the other party. Besides that, the principles that must be carried out by

banks in conducting their business are: The principle of trust, the principle of confidentiality, the principle of prudence and the principle of knowing your customer as a prevention of money laundering through suspicious transactions by customers (Saliman, 2005, 2005).

From a legal point of view, the relationship between the bank and the customer can be divided into two forms: contractual and non-contractual relationships. The relationship between the bank and the customer is based on the two most related elements called law and trust. A bank can only carry out activities and develop its business, if the public "believes" to place their money in the existing banking products at the bank. Based on this public trust, banks can mobilize funds from the public to be placed in their banks and banks will provide banking services (Bako, 1994; Roni, 1995).

The most important and common relationship between a bank and a customer is a contractual relationship. This applies to almost all customers. For debtor customers, the contractual relationship is based on a contract made between the bank as the creditor (fund provider) and the debtor (fund borrower). The contract law that forms the basis of the bank's relationship with the debtor customer originates from the provisions of the Civil Code regarding contracts (third book), because according to article 1338 paragraph (1) of the Civil Code that all agreements made legally have the same force as the law for both parties (Ramadhan & Asih, 2021; Yulita et al., 2021).

The formal relationship between the customer and the bank is contained in forms that have been filled in by the customer and approved by the bank. The forms contain requests or orders or power of attorney at the bank. These forms are generally made by banks. The form will point to each other terms relating to the transaction desired by the customer. Each of these forms is essentially part of an inseparable unit (Widiyono, 2006). Customers who fill out application forms, orders or power of attorney to banks are basically a follow-up of public trust in banks. The customers manifest their trust in the form of submitting a trusted application. The relationship between the bank and the customer often refers to the enactment of comprehensive provisions and these provisions are stated as an integral part of the application.

Customer's Data

According to Article 1 paragraph 28 of Law Number 7 of 1992 concerning Banking (Banking Law) as amended by Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking that bank secrecy is everything related to information about depositors and their deposits.

Explicitly, the obligation of a bank to keep the information of its customers secret is regulated in Article 40 paragraph (1) of Law 10/1998, but what is required to be kept secret is limited to depositors and their savings, except in cases referred to in Articles 41-44 in cases such as for tax purposes based on the request of the Minister of Finance; for the settlement of bank receivables that have been submitted to the State Receivables and Auction Agency, the State Receivables Affairs Committee; for the benefit of justice in criminal cases; in civil cases between banks and their customers; in the context of exchanging information between banks; at the request, approval or power of attorney from the depository customer made in writing. Article 3 paragraph (1) of PBI 2/19/2000 confirms that the implementation of the provisions for requesting bank secrecy in relation to the above issues requires first obtaining written orders or permission to disclose bank secrets from the leadership of Bank Indonesia. If a permit is not obtained, then of course it can be punished under Article 47 paragraph (1) and paragraph (2) of Law 10/1998 threatened with imprisonment for at least 2 years and a maximum of 4 years and a fine of at least IDR 10 billion and a maximum of IDR 200 billion. This also violates Article 47 paragraph (2) of Law 10/1998 where Members of the Board of Commissioners, Directors, bank employees or other Affiliated Parties who deliberately provide information that must be kept confidential according to Article 40, are punishable by imprisonment for at least 2 years and a maximum 4 years and a fine of at least IDR 4 billion and a maximum of IDR 8 billion.

Leakage of customer data by bank employees is a violation of bank secrecy. The violation of bank secrecy, even though it is carried out by a bank employee, can be accounted for by the bank as a party that is obliged to maintain the confidentiality of customer data. Banks as financial services can be subject to sanctions based on Article 53 POJK Number 1/POJK.07/2013 concerning consumer protection in the financial services sector. Sanctions that can be given to banks as financial service actors who violate the provisions in the Financial Services Authority Regulation are subject to administrative sanctions, including: a. Written warnings, b. Fines - obligation to pay a certain amount of money, c. Restrictions on business activities, c. Freezing business activities, d. Revocation of business activity permits.

Method

This research uses a type of prescriptive empirical juridical research with a legal and case approach which is a type of research that combines empirical methods and a legal approach in studying legal issues. This study aims to understand and analyze the applicable legal regulations and how the law is applied in concrete cases. In prescriptive empirical juridical research with legal and case approaches, it is important to maintain a balance between legal analysis and empirical understanding. A combination of the two will provide a more comprehensive insight into the research topic you are researching.

Results and Discussion

Values There are two causes of customer data leakage: internal and external. Internal factor typically leaks customer data because dishonest employees illegally sell the data to parties who want it. While with the external factor, the data leak is caused by customers who used debit or credit cards for too many non-cash transactions at various retailers and online stores (Butler & Madhloom, 2016; Mahaputra & Saputra, 2021; Winner, 2022). Security of customer data in the banking industry is a major concern. This is due to the fact that customer data from banks typically contains personal and sensitive information that can be used fraudulently or for identity theft. In this day and age, when data leaks are common, customer data protection requires special attention. Banks, as one of the financial institutions that handle money and public financial transactions, are required to guarantee the highest level of data security to their customers. In addition, banks have an ethical obligation to safeguard the privacy of their customers by safeguarding customer data. As a result, the banking industry continues to strive for service excellence by safeguarding customer data from unauthorized

access through appropriate security measures.

The application and advancement of information technology in banking services is a top priority in the current digital era. This innovation is supposed to expand the efficiency, viability and proficiency of banking tasks in serving clients. Telebanking, integrated computer systems that connect units, and ATMs are some of the technologies used. Cybercrimes that target banking data security systems are especially intertwined with the development of increasingly sophisticated technology. Cybercrime in the banking industry is a relatively new type of crime that stands out from other types of crime in general. Some of the characteristics of this cybercrime are: Non-violence, Minimal physical contact, Using sophisticated equipment and technology, Utilizing global telecommunications networks, media and informatics.

Cybercrime in the banking sector has taken many forms over the past decade. Some of them are carding, typosite, sniffing (scam) and phishing. The victim's credit card information is illegally obtained by the carding perpetrator, who then uses the credit card to shop online (forgery). This mode happens because of frail financial information security frameworks, client carelessness and feeble verification frameworks used to distinguish the personality of online item orderers. Cybercrime in the financial business that is in many cases found connected with Visa information robbery is phishing. The perpetrator targets the 4-digit credit card number and the PIN number in this mode. The information is utilized by the culprit to execute in the interest of the client. In the beginning, the perpetrator will call the victim pretending to be a bank employee to update the personal credit card information. In addition, criminals frequently use transaction modes in fake online stores and skim at ATM or EDC machines.

The following are several types of customer data that have the potential to leak: Personal information such as name, address, telephone number, date of birth and identity number. Financial data such as bank account information, transaction records and credit card details. Health information such as medical history, laboratory test results and data on drugs consumed. Online account information such as usernames and passwords. Other personal data such as voice or video recordings, photos and personal documents. All types of data can be used by irresponsible parties to commit crimes such as identity theft, fraud or data logging. Therefore, it is important for the banking industry to take appropriate security measures to protect customer data from leaks.

This data leak from customers could have come from either internal or external sources, like employees accidentally sending sensitive information online or human error. Malware or intruders who entered via email, internet downloads, or infected programs are additional causes of this data leak. When it comes to providing services and earning the trust of customers, the banking industry is concerned about the security of customer data. This data security protection focuses on human resource integrity-supported procedures and implementation.

Following are some of the efforts and ways in which the banking industry ensures the security of customer data: 1) Using encryption to keep customer data secure when sent or stored. Encryption is the process of turning data into a code that cannot be read by someone who does not have the encryption key. 2) Using a multi-factor authentication system to ensure only authorized persons can access customer data. For example, using a combination of secret codes, card tokens and fingerprints to verify user identity. 3) Maintaining the physical security of customer data by storing the data on well-protected servers and using strict security procedures at data storage centers. 4) Conducting regular security audits to ensure the security system is still effective and address security weaknesses that may occur. 5) Providing data security training to banking employees so that they understand the importance of customer data security and how to maintain data security. 6) Signing confidentiality agreements with employees, vendors and partners to ensure that customer data will not be disclosed to unauthorized parties. 7) Providing a data leak reporting mechanism for customers so that customers can immediately report any leakage of their personal data (Choiriyah, 2019; Komarudin & Hidayatullah, 2021; Wafa, 2017).

It is believed that the bank's obligation to maintain customer confidentiality is weaker when third parties can easily obtain personal data about customers through dishonest bank employees and freely trade it. One of the cases that happened was the offer of client information by a client information deals network through a site which was uncovered on August 23, 2021 at Bank Syariah Indonesia (BSI) in the Lhokseumawe region. Since 2020, the suspect has been collecting customer data from bank marketing. It was discovered that the case began with a rise in public complaints about individuals offering credit cards, insurance, or other products over the phone. It turned out that the caller claimed to be a telemarketing officer for a company that purchased bank customer data from the suspect, despite the fact that the owner of the number never felt he was giving the number to the caller. The suspect obtained customer data by exchanging information with bank marketing division employees. The suspect sold customer data through the website at prices varying from IDR. 350,000, - up to IDR. 1,000,000, - a thousand customer data was sold for IDR. 350,000, - while a package of 100 customer data was sold for IDR. 1,000,000. This caused material losses to customers, considering that data from customers can easily be known by the general public who are not interested.

Banks as financial service institutions and payment system providers, as stipulated in the Financial Services Authority Regulation Number 1/POJK.07/2013 concerning consumer protection in the financial services sector and Bank Indonesia Regulation Number 16/I/PBI/2014 confirms that, banks must implement consumer protection with the principle of confidentiality and security of personal data. This is a legal obligation for banks on the basis of safe deposit agreements with customers and constitutes bank secrecy provisions required by banking law in banking business activities. At Bank Syariah Indonesia in Lhokseumawe City there was also a leak of customer data (Interview, Haris BSI Lhokseumawe employee, October 27, 2022). This is due to the negligence of the customer, the customer clicks on the link carelessly and inputs or submits the OTP code to someone else. If there are parties acting on behalf of BSI, then official calls are only via 14040, not personal numbers and if contacted via WhatsApp or other social media, make sure the account is verified in the form of a blue tick (Interview, Ramli BSI Lhokseumawe, 28 October 2022).

Banks as actors of financial services can be held accountable in the event that there are mistakes made by bank employees that are detrimental to bank customers. This is also related to the principle of vicarious liability. The corporation in this case is the bank responsible for the actions committed by its employees or parties who are responsible and who have ties with the bank. Mistakes made by these employees are attributed and borne by the bank. At the BSI Lhokseumawe bank, cases caused by external parties, the procedure is to visit Customer Service or contact the call center to freeze accounts, ATM cards and others. Then a follow-up will be carried out on the track record of the transaction, if the track of the flow of money is known then the lost amount will come back again, but if not, then it is the customer's own fault as a result of filling in an illegal link (Interview, Haris BSI Lhokseumawe, November 3, 2022).

Conclusions

Every At Bank Syariah Indonesia Lhokseumawe, there was also the data leak. This is caused by internal and external factors. The cause of internal leakage was caused by Bank Syariah Indonesia's employees, while unscrupulous parties who commit various forms of fraud in order to profit from customer data are to blame for external factors. For this kind of situation, Bank Syariah Indonesia is responsible for activities that are unfavorable to the client and if there is a loss of customer funds the bank will compensate the customer for the loss.

References

Bako, R. S. H. (1994). *Hubungan bank dan nasabah terhadap produk tabungan dan deposito: suatu tinjauan hukum terhadap perlindungan deposan di Indonesia dewasa ini*.

Butler, N., & Madhloom, O. (2016). Teaching company law to business students: An effective framework. *Law Teacher*, *50*(2). https://doi.org/10.1080/03069400.2015.1045260

Choiriyah, C. (2019). Hukum Perbankan dan Perasuransian Indonesia Dalam Perspektif Hukum Islam. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, *6*(3). https://doi.org/10.15408/sjsbs.v6i3.11532

Dr Jamin Ginting S.H. M.H. (2017). Pengertian dan Sejarah Perbankan di Indonesia. *Perbankan Indonesia*, *1*(Perbankan).

Husen Sobana, H. D. (2016). *Hukum Perbankan di Indonesia*. Pustaka Setia.

Komarudin, P., & Hidayatullah, M. S. (2021). Alur Legislasi dan Transformasi Hukum Perbankan Syariah di Indonesia. *Mizan: Journal of Islamic Law*, *5*(1). https://doi.org/10.32507/mizan.v5i1.868

Mahaputra, M. R., & Saputra, F. (2021). Application of Business Ethics and Business Law on Economic Democracy that Impacts Business Sustainability. *Journal of Low Politic and Humanities*, *1*(3).

Moleong, L. J. (2019). Moleong, " Metodologi Penelitian Kualitatif Edisi Revisi". Bandung : Remaja Rosdakarya. *PT. Remaja Rosda Karya*.

Ramadhan, M. Z. J., & Asih, V. S. (2021). Studi Komparatif: Kualitas Layanan Mobile Banking BRI Syariah dan Bank Syariah Indonesia. *Indonesian Journal of Economics and Management*, *1*(3). https://doi.org/10.35313/ijem.v1i3.3492

Roni, S. H. B. (1995). *Hubungan Bank dan Nasabah Terhadap Produk Tabungan dan Deposito*. Jakarta: Citra Aditya Bakti.

Saliman, A. R. (2005a). Hermansyah, Ahmad jalis. *Hukum Bisnis Untuk Perusahaan Teori Dan Contoh Kasus*.

Saliman, A. R. (2005b). Hukum bisnis untuk perusahaan. *Teori Dan Contoh Kasus, Jakarta: Prenada Media Group*.

Sri Wahyuni, & Kurniawan, R. R. (2022). Sejarah Perbankan Syariah Di Indonesia. *Al Ibar*, *1*(8.5.2017).

Wafa, M. A. (2017). HUKUM PERBANKAN DALAM SISTEM OPERASIONAL BANK KONVENSIONAL DAN BANK SYARIAH. *Kordinat: Jurnal Komunikasi Antar Perguruan Tinggi Agama Islam*, *16*(2). https://doi.org/10.15408/kordinat.v16i2.6441

Widiyono, T. (2006). *Aspek Hukum Operasional Transaksi Produk Perbankan di Indonesia: Simpanan, Jasa dan Kredit*.

Winner, M. (2022). THE DUTY OF CARE AND BUSINESS JUDGMENT RULE IN AUSTRIAN COMPANY LAW. *Acta Universitatis Carolinae Iuridica*, *68*(3). https://doi.org/10.14712/23366478.2022.32

Wulandari, Y., & Ghozali, M. (2019). Sejarah Perkembangan Hukum Perbankan Syariah Di Indonesia Dan Implikasinya Bagi Praktik Perbankan Nasional. *… Dan Perbankan Syariah*.

Yulita, Y., Apriza, M., Wulandari, S., Isnaini, D., & Arisandy, Y. (2021). Management level of using digital services Bank Syariah Indonesia (BSI) KCP ipuh. *BIMA Journal (Business, Management, & Accounting Journal)*, *2*(2). https://doi.org/10.37638/bima.2.2.200-211

Republik Indonesia Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi

Republik Indonesia Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan

Republik Indonesia Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah

Republik Indonesia Undang-Undang Nomor 10 Tahun 1998 sebagai perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Qanun Aceh Nomor 11 Tahun 2018 tentang Lembaga Keuangan Syariah.

Qanun Aceh Nomor 8 Tahun 2014 tentang Pokok-Pokok Syariat Islam.