INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

A Cyber Security And Protection Of Privacy Rights In E-Commerce Transactions

Helma Widya[1], Hermansyah Alam[2]
[1]Politeknik LP3i Medan, North Sumatera, Indonesia, [2]Universitas Islam Sumatera Utara, Medan, North Sumatera, Indonesia

Article Info
Keywords:
Cybersecurity,
Privacy Rights,
E-Commerce,
Data Protection,
Digital Transactions.

ABSTRACT
The rapid growth of e-commerce has revolutionized the way businesses and consumers interact, providing convenience and accessibility. However, this advancement also presents significant challenges in cybersecurity and the protection of privacy rights. This paper examines the key cybersecurity threats in e-commerce transactions, including data breaches, identity theft, phishing attacks, and unauthorized access. It also explores the legal and regulatory frameworks designed to protect consumer privacy, such as GDPR, CCPA, and Indonesia's Personal Data Protection Law. The study analyzes existing security measures, including encryption, multi-factor authentication, and blockchain technology, to enhance transaction security and safeguard user data. Additionally, the research highlights the role of businesses in ensuring compliance with privacy laws and implementing best practices in data protection. The findings suggest that while technological solutions play a crucial role in mitigating cybersecurity risks, consumer awareness and regulatory enforcement are equally important in strengthening e-commerce security.

Corresponding Author:
Helma Widya
Politeknik LP3i Medan, North Sumatera, Indonesia
Helmawidya140969@gmail.com

INTRODUCTION

Naturally, all human activities and behavior change in accordance with technological advances, the aim of which is to make life easier.Along with the development of people's needs in the world, information technology plays an important role, both now and in the future. Globalization has become a driver of the birth of the era of information technology development that can be accessed in all countries.

The development of information technology from various countries encourages people to follow and accept it, one of which is the products resulting from this information technology, such as computers, ATMs (Automatic Teller Machines), facilities for building the internet and the formation of a non-financial institution, as well as a financial institution that is a place for people to place their funds as a form of savings, trust and provide all information or confidential information data belonging to them and obtain credit facilities as a form of loan.

In Indonesia, there are 2 (two) types of banks known, namely conventional banking and Islamic banking where all banking activities have been regulated in the provisions of

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

laws and regulations or based on Islamic Law (Sharia Principles). One of the prominent differences between conventional banking and Islamic banking is seen in the benefits obtained by customers, namely the existence of bank interest and the absence of bank interest or profit sharing from every transaction carried out by the community in Islamic banking.

Basically, a bank is a financial institution or business entity that collects funds from the community and distributes them to the community in order to improve the community's standard of living.This means that banks are used as intermediaries in public finance (financial intermediaries) and provide banking services for those who have excess funds (surplus of funds) and those who need and lack funds (lock of funds). The main activities are known as funding, lending, and service.The three main activities above are carried out based on a storage agreement or contract or an agreement or contract between the bank and the depositor.

Based on this contract, a contractual relationship arises between the bank and the customer which is based on the principle of trust (fiduciary principle) and the principle of bank confidentiality (confidential principle).6The existence of the fiduciary principle has consequences so that banks do not only pay attention to their own interests, but must also pay attention to the interests of depositors. Including the bank's obligation to pay attention to the interests of its customers which is based on the confidentiality principle.7The principle of confidentiality is a principle that requires or obliges banks to keep confidential everything related to data, information and statements about customers, both their financial situation and personal information, so as to create a relationship of trust (fiduciary relationship) between the bank and its customers.

From the interview results with Mr. Septianto Pane, as Branch Operation and Service Manager at Bank Syariah Indonesia Pematang Siantar Branch Unit, explained that customer information or data that must be kept confidential by the bank can be in the form of name, address, date of birth, age, telephone number, and mother's name for individuals. Meanwhile, corporate or company information data that must be kept confidential by the bank can be in the form of company or corporation name, address, telephone number, board of directors and board of commissioners including their identities, namely KTP (Resident Identity Card/passport/residence permit) and the composition of shareholders.9In practice, many people complain about the many offers of products in the financial services sector via short messages/SMS and e-mail or via telephone calls. The products offered are in the form of insurance, additional credit card facilities for customers who already have credit cards and online or offline money lending.

The existence of freelance telemarketers who admit that their company has collaborated with a bank where customers store their funds has caused some people as customers of the bank to easily trust them and some other customers have suspicions about the bank because they have provided information or personal information data to other parties without the customer's consent.Thus, irresponsible individuals can easily access customer personal information or data to gain maximum profits.

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Literature Review

Provisions Concerning Banking Confidential Data Reviewed From Law Number 21 of 2008 concerning Islamic Banking

Article 1 number 1 of Law Number 21 of 2008 concerning Sharia Banking explains that a Sharia Bank is a bank that carries out its business activities based on Sharia Principles and according to its type consists of Sharia Commercial Banks and Sharia People's Financing Banks.1Islamic General Bank is a Sharia Bank that in its activities provides services in payment traffic. The implementation of banking business activities must be based on legal principles in the banking sector.2One of the important principles in banking business activities is the Fiduciary Principle, which states that banking business is based on a relationship of trust between the bank and its customers, and the Confidentiality Principle is a principle that requires or obligates banks to keep confidential everything related to information and information data regarding bank customers according to banking standards and their deposits.

Customer confidentiality data according to banking standards is confidential banking data. Article 1 number 14 of Law Number 21 of 2008 concerning Sharia Banking explains that bank secrecy is everything related to information about depositors and their deposits and Investor Customers and their Investments. Depositors are customers who place their funds in Sharia Banks and/or UUS in the form of deposits based on wadi'ah contracts or other contracts that do not conflict with Sharia Principles between Sharia Banks or UUS and the Customer concerned in the form of demand deposits, savings, or other forms that are equated with that. Meanwhile, Investor Customers are customers who place their funds in Sharia Banks and/or UUS in the form of investments based on mudharabah contracts or other contracts that do not conflict with Sharia Principles between Sharia Banks or UUS and the Customer concerned in the form of deposits, savings and/or other forms that are equated with that. In general, deposit customers or investor customers known in the banking sector are individuals and corporations (companies or other legal entities) domiciled in Indonesia.

The form of confidential data regarding customers according to banking for individuals is personal identity according to KTP (Resident Identity Card), the amount of finances/investments, types of savings, whether savings in the form of checking and savings or investments in the form of deposits and savings or those that are equivalent to that, customer account number, savings book, ATM password, transaction data carried out by customers every day, customer bank statements, loan amount, type of loan, loan term, cooperation agreement between the Customer and the Sharia Bank based on the mudharabah or wadi'ah contract or other contracts that do not conflict with sharia principles, as well as interest/profit sharing for the Bank and the Customer. This also applies to corporations or companies with additional confidential data in the form of the founder's identity, namely KTP (Resident Identity Card) for Indonesian citizens and Passport/Residence Permit for Foreign Citizens and the Company's Articles of Association.

Furthermore, confidential data regarding customers at the Bank implements the bank's principle of prudence in terms of providing credit or financing based on sharia

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

principles as a form of bank accountability to third parties. In other words, this principle is applied by the bank's affiliated parties to analyze customers before credit or financing based on sharia principles is provided, the aim of which is to avoid problematic and stalled credit or financing, as well as the Bank's main principle in maintaining and improving the level of operational health and all business activities in general banking and sharia banking. The principle of prudence is known as the 5 C's analysis of Credit which consists of assessing the customer's character, capacity, capital and business prospects (condition of economy).

In Indonesia, disclosing confidential data regarding depositors or investor customers in Islamic banking can be considered a crime against bank secrecy or official secrecy.9However, on the other hand, disclosing confidential data regarding depositors or investor customers in Islamic banking is permitted if it is for the purposes of criminal tax investigations by attaching written permission from the head of Bank Indonesia, the interests of the courts in criminal cases by attaching written permission from Bank Indonesia, upon request and approval or power of attorney from depositors made in writing, the interests of civil cases between the Bank and its Customers, in the context of exchanging information between banks, upon request for approval or power of attorney from Customers.

Depositors or Investor Customers made in writing, the interests of the legal heirs of the depositor when the depositor has died. As well as parties who feel disadvantaged by the information provided by the Bank. Thus, if confidential data regarding depositors or investor customers in Islamic banking is not in accordance with the provisions of Law Number 21 of 2008 concerning Islamic Banking and is open without the customer's knowledge, then the law enforcement given for such legal acts is in the form of administrative sanctions, imprisonment and fines as regulated in Article 56- Article 66 of Law Number 21 of 2008 concerning Islamic Banking.

Customer Information as Banking Confidentiality Data at Bank Syariah Indonesia, Pematang Siantar Branch Unit

In general, the definition of an Islamic Bank is a bank that its operation is based on Islamic sharia principles. Other terms used to refer to Islamic Bank entities other than Islamic Bank itself are Interest-Free Bank, Riba-Free Bank (Lariba Bank), and Sharia Bank.11Legally, Indonesia refers to Islamic Banks using the term “Sharia Bank” or “Bank based on Sharia Principles”. The main principle of Sharia Banks is the implementation of business activities on the basis of equality, fairness, transparency, the formation of mutually beneficial partnerships, and the obligation to obtain profits in a halal manner.

In its development, on February 1, 2021, 3 (three) Sharia Commercial Banks owned by state-owned banks, namely PT. Bank Syariah Mandiri, PT. Bank Rakyat Indonesia Syariah, and PT. Bank Negara Indonesia Syariah have officially obtained permission from the Financial Services Authority to carry out a business merger or merger into Bank Syariah Indonesia with the stock code used remaining BRIS.However, the operation of Bank Syariah Indonesia is still in accordance with the objectives and operational activities of the previous Sharia General Bank. Bank Syariah Indonesia also carries out all post-merger business activities at the head office, branches and sharia business units (UUS) previously owned by

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Bank Syariah Mandiri, BRI Syariah, and BNI Syariah and the legal basis used by Bank Syariah Indonesia still covers the scope of Law Number 21 of 2008 concerning Sharia Banking along with the laws and regulations of Bank Indonesia as implementing laws and regulations In Indonesia, Sharia Banks adhere to the theory of relative or relative bank secrecy, which means that banks have an obligation to disclose bank secrecy by using the principle of proportionality, looking at the circumstances, considerations and prioritizing certain interests based on applicable laws and regulations.[16]In essence, banks and affiliated parties of banks are required to keep confidential information about Depositors and their Deposits and Investor Customers and their Investments. This means that there are prohibitions for Islamic banking to provide information or information about financial data or personal data of depositors, as well as financial data or personal data and the amount of investment from investor customers to anyone including other customers and affiliated parties of Islamic banks.

However, it does not mean that Islamic banks do not have any bank transparency at all because transparency is also needed for the community of funders, investors, and the government to be able to know the condition of the bank's prospects. Islamic banks represented by the Bank's Board of Directors with permission from the Head of Bank Indonesia are obliged to provide or open customer information or information that is a secret of Islamic banks for the purpose of the interests of the state, law, and society.

The dissemination of information or data regarding customers is a criminal act which is grouped into two groups, namely violation of bank secrecy as a civil violation which arises from the contractual relationship between the bank and the customer, and the violation of bank secrecy as a criminal violation. Therefore, any person or legal entity or affiliated party of Bank Syariah Indonesia who intentionally without a written order or permission from Bank Indonesia, without the knowledge of the customer and forces Bank Syariah Indonesia, UUS or affiliated parties to provide customer information or information that should be kept confidential shall be subject to sanctions in the form of administrative sanctions, imprisonment and fines as stipulated in Article 56 - Article 66 of Law Number 21 of 2008 concerning Sharia Banking.

With the presence of Bank Syariah Indonesia, all customer information or statements that are bank secrets are in the ART (household budget) of Bank Syariah Indonesia and make it easier for customers to get all superior sharia banking services under one roof.21Bank Mandiri, which is the driving force or chairman of Bank Syariah Indonesia, is now requesting that every customer at each bank previously provide information regarding personal data or confidential banking data in order to audit and re-check the completeness of savings and investments owned by customers.

The form of customer information as banking confidentiality data at Bank Syariah Indonesia Pematang Siantar Branch Unit is in the form of personal identity according to KTP (Resident Identity Card), telephone number, mother's name, email address, home address, savings book and verification code or OTP to access Customer mobile banking for individuals, as well as additional information in the form of the founder's identity, namely KTP (Resident Identity Card) for Indonesian Citizens or Passport/Residence Permit for

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Foreign Citizens, company email address, shareholder composition, names of the company's board of directors and board of commissioners and types of business fields run by the company along with the company's business license for corporations or companies.

Legal Basis for Customer Confidentiality Data Reviewed from the Law Number 19 of 2016 concerning Electronic Information and Transactions

According to Article 1 number 2 of Law Number 19 of 2016 concerning Information and Electronic Transactions, it is explained that electronic transactions are legal acts carried out using computers, computer networks, and/or other electronic media such as mobile phones. Meanwhile, information technology is a technique for collecting, preparing, store, process, announce, analyze, and/or disseminate information as stated in Article 1 number 3 of Law Number 19 of 2016 concerning Information and Electronic Transactions. If customer confidentiality data according to banking standards is stored in information technology and electronic media, then banking provides convenience and comfort for customers to access their financial transactions anytime and anywhere through an electronic system in the form of electronic documents.

The phenomenon of information technology development encourages conventional banking and Islamic banking to provide banking products and financial services based on information technology (financial technology) or digital banking. Then, in order for the quality of banking products and financial services to enter the era of healthy digital banking services, it is necessary to increase bank capabilities followed by alignment of targeted business strategies.

From the results of the interview with Mr. Septianto Pane, as Branch Operation and Service Manager at Bank Syariah Indonesia Pematang Siantar Branch Unit, he stated that there are several digital banking financial services that are currently developing at Bank Syariah Indonesia (BSI) Pematang Siantar Branch Unit, namely as follows:Internet bankingis a digital banking transaction service where customers can carry out banking transactions (financial and non-financial) via a computer connected to the internet network by filling in their personal and financial information such as user ID, login password, email, ATM PIN, BSI Net authorization and customer TAN on the Bank Syariah Indonesia website page.https://bsmnet.syariahmandiri.co.id/cms/.The types of internet banking transactions are:

a. Fund Transfer;
b. Checking Balance Information, Account Mutations, and Foreign Currency Exchange Rate Information;
c. Make Bill Payments such as credit cards, telephone, mobile phones, and electricity;
d. Can make purchases such as topping up telephone credit, airline tickets and shares.

Phone Bankingis a digital banking transaction service where customers can conduct banking transactions via telephone by contacting the Bank Syariah Indonesia contact center at Call Center 14040 or the Bank Syariah Indonesia Pemantangsiantar Branch Office Telephone Number at (0622) 7430146. In this case, the bank has provided special staff who will carry out customer transactions or automatic programs that can interact with customers to carry out customer transactions 24 hours a day, every day. The types of

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

transactions that can be carried out by customers via phone banking include fund transfers, checking information balance, account transfers, credit card bill payments, telephone, mobile phone, electricity and insurance;

SMS Bankingis a digital banking transaction service where customers can send a Short Message Service (SMS) format to the Bank Syariah Indonesia telephone number or use the BSI Mobile application that has been installed by the bank on the customer's cellphone where when the customer is asked to verify the data there will be a reactivation code sent by the bank to the customer via BSI Mobile SMS. The types of transactions that customers can do via SMS Banking include fund transfers, checking balance information, account transfers, credit card payments, and purchasing top-up credit;

Mobile Bankingis a digital banking transaction service where customers can access banking transactions directly to applications that have a higher level of sophistication. It is known that the Bank cooperates with cellular operators, so that in the SIM Card (customer's cellular chip card) a special program has been installed to be able to carry out banking transactions and is Global for Mobile Communication (GSM) which means it can be accessed anywhere and anytime through the Bank Syariah Indonesia Mobile Banking application using a cellular network or Wireless Fidelity (WiFi). However, in practice, there is often misuse, widespread and violation of the bank's obligations in terms of keeping confidential personal and financial information and data of customers through information technology and electronic media caused by 2 (two) factors, namely Internal Factors originating from the bank or other bank affiliated parties who seek their own profit by using customer personal data secretly and without the customer's knowledge to open a savings book at one of the banks that functions as a hiding place or disguise the origin of assets obtained from criminal acts (money laundering), selling bank customer data to the public at varying prices, copying and imitating customer signatures that have been stored in electronic documents that appear to function as a form of approval from the customer to transfer some or all of the customer's finances to the account of the bank or other bank affiliated parties, deliberately editing the nominal transaction income and expenses of customers that do not correspond to the truth in mobile banking, and not fulfilling the provisions in the exception to opening bank customer confidentiality data as stated in Article 42 - Article 49 of Law Number 21 of 2003. 2008 concerning Islamic Banking. External Factorsnamely from customers and third parties outside of customers and banks. Usually this factor is caused by customer negligence or the existence of third parties who hack (hacker) customer confidentiality data from internet banking, phone banking, SMS banking, mobile banking, and ATM machines. The form of customer negligence is the customer's habit of making many transactions at merchants (trading goods and services) in shopping centers, restaurants and hotels, as well as electronic commerce transactions (e-commerce). In this case, the seller uses an EDC (Electronic Data Capture) machine as a means of payment between the customer and the seller by swiping the customer's ATM (Automatic Teller Machine) card twice (double swipe) on the machine or entering the credit or debit card serial number along with other verification information such as e-mail,

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

telephone number, PIN, and verification code received by the customer via SMS on one of the e-commerce.

Unwittingly, the EDC (Electronic Data Capture) machine and the e-commerce application have a capture tool that records and stores all customer confidentiality data starting from the transaction amount to the password entered in the payment method. In addition, ordinary customers are often easily influenced by all the attractive offers from third parties who claim to be banks through phone banking and SMS banking so that they easily provide personal information and customer information along with their savings. Thus, the forms of misuse or open and widespread ways of customer confidentiality data through electronic media, the exception is legal protection for the community, along with criminal sanctions given to perpetrators of criminal acts, which have been explained in Article 31, Article 40, Article 43, Article 45, Article 45 A, and Article 45 B of Law Number 19 of 2016 concerning Electronic Information and Transactions.

METHOD

Bank secrets are customer confidentiality data or information and information about depositors or investor customers is inputted through an integrated banking information system so that supervision by BI and OJK is needed. The coordination between OJK and BI has resulted in several regulations for supervision of confidential data of depositors or investor customers in the field of Islamic banking, such as containing the Requirements and Procedures for Giving Written Orders or Permissions in the context of Opening Bank Secrets, instructions for implementing and applying the principle of Confidentiality, as well as parties authorized to maintain the Security of Consumer Data and/or Personal Information as a form of protection for depositors or investor customers who are consumers in the financial services sector.

This aims to ensure that banks remain trusted by the public, customer confidentiality data is kept safe and does not cause losses to customers and bank operations remain healthy. The requirements for granting written permission to open customer confidentiality data according to banking standards have been regulated in PBI Number 2/19/PBI/2000 concerning Requirements and Procedures for Granting Written Orders or Permissions to Open Bank Secrets include the following:

1. In order to open bank secrets for the purpose of tax audit and investigation, it is necessary to meet the requirements that the opening must be accompanied by a written request from the Minister of Finance, in which the written request must state the name of the tax official, the name of the depositor or investor customer of the taxpayer whose information is desired, the name of the bank office where the customer has savings or investments, the information requested, and the reasons for the need for information and information regarding the depositor or investor customer. However, if the need is to implement the provisions of other tax laws and regulations, the tax authorities can directly request information or evidence from the bank regarding the financial condition of its customers;

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

2. In order to reveal bank secrets for the purpose of settling bank receivables that have been submitted to the State Receivables and Auctions Agency/State Receivables Committee (BUPLN/PUPN), it is necessarythe conditions that the opening must be accompanied by a written request from the Head of the State Receivables and Auctions Agency/Chairman of the State Receivables Committee, in which the written request must state the name and position of the BUPLN/PUPN official, the name of the debtor customer concerned, the name of the bank office where the debtor customer has savings or investments, the information requested, and the reasons for the need for information and statements regarding the depositor or investor customer;
3. In order to reveal bank secrets for the benefit of public justice or outside public justice in criminal cases, it is necessary to have conditions that the opening must be accompanied by a written request from the Chief of the Indonesian National Police, the Attorney General of the Republic of Indonesia or the Chief Justice of the Republic of Indonesia, in which the written request must state the name and position of the police, prosecutor or judge, the name of the suspect or defendant, the name of the bank office where the suspect or defendant has savings or investments, the information requested, the reasons for the need for information and information regarding the depositor or investor, and the relationship of the criminal case in question to the information and information required.

Meanwhile, opening customer confidentiality data according to banking standards intended for the purpose of exchanging information between banks, requests, approvals or powers of attorney from Depositors or Investors, and requests from legal heirs of Depositors or Investors who have died must meet the requirements, namely the Bank's Board of Directors or PUJK (Management of Financial Services Business Actors) must obtain written approval stated in the form of a choice of agree or disagree and/or approval required by laws and regulations from consumers as depositors or investor customers, then the written approval is given to a third party.

In addition, the Board of Directors of the Bank or PUJK must ensure or remind third parties not to provide and/or use Consumer Personal Data and/or Information for purposes other than those agreed between the Board of Directors of the Bank or PUJK and third parties. The above requirements also apply to the Board of Directors of the Bank or PUJK in the context of exchanging information between banks or with insurance companies, civil cases between banks and their customers, namely the Board of Directors of the Bank providing information and customer information data to the court, there is a request, approval or power of attorney from the depositor or investor customer, in the case of a depositor or investor customer who has died so that the heirs of the depositor or investor customer concerned has the right to obtain information and data regarding the savings of the depositor or investor customer, and in the event that there is a party who feels disadvantaged because the information provided by the Bank is incorrect, so that the person who feels disadvantaged has the right to know the contents of the information and request corrections if there are errors in the information and information provided.

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

The difference in legal protection for Customers in the Sharia Banking Law and the Conventional Banking Law lies in the party that carries out bank guidance and supervision. The establishment of the deposit insurance institution (LPS) and the implementation of the provision of guarantees are carried out by the Minister of Finance based on a Presidential Decree and forming a government guarantee implementation unit within the Ministry of Finance as referred to in Article 5 of Presidential Decree Number 17 of 2004 concerning amendments to Presidential Decree Number 26 of 1998 concerning Guarantees for Payment Obligations of General Banks. Then, repressive legal protection, namely protection law that aims to resolve disputes between banks and customers including disputes regarding the disclosure of confidential bank data without customer consent through general courts and state administrative courts. In the Banking Law, the form of repressive legal protection is to resolve disputes by imposing administrative sanctions and criminal provisions as referred to in Article 46 - Article 52 of Law Number 10 of 1998 concerning Banking. Meanwhile, the form of legal protection for Customers provided by Islamic Banks is in the form of preventive legal protection, namely legal protection carried out through the efforts of the role and opinion of Bank Indonesia in the framework of fostering and supervising Islamic banks and UUS. This protection aims to prevent disputes and before a definitive government decision is stated. The provisions regarding the fostering and supervision of Islamic banks and UUS carried out by Bank Indonesia have been regulated in Article 50 - Article 54 of Law Number 21 of 2008 concerning Islamic Banking. Then, repressive legal protection, namely legal protection aimed at resolving disputes between banks and customers including disputes over the disclosure of confidential bank data without the customer's consent through religious courts, the settlement of disputes is carried out in accordance with the contents of the contract, and must not conflict with Sharia Principles, and impose sanctions administrative and criminal provisions as referred to in Article 56 – Article 66 of Law Number 21 of 2008 concerning Sharia Banking.

RESULT

Preventive Efforts Against Customers Regarding Information Given as Banking Confidentiality Data at Bank Syariah Indonesia, Pematang Siantar Branch Unit According to Law Number 21 of 2008 concerning Sharia Banking

The weak position of customers makes customers need legal instruments that will provide a balanced position between business actors and consumers while providing a sense of security for consumers (customers). One form of legal protection that banks can provide to customers is in the form of preventive efforts.

In general, the handling of problematic financing can be done through preventive efforts and repressive/curative efforts. Preventive efforts are carried out by the bank since the customer submitted the financing application, the implementation of accurate analysis of financing data, the creation of correct financing agreements, and the binding of collateral which guarantees the interests of the bank, up to monitoring or supervision of the financing provided. Thus, customer data or information contained in the financing contained in an agreement must be kept confidential by the bank.

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Transparency in the use of personal data submitted by customers to banks requires legal protection so that the personal rights of customers who have a relationship with the bank and the use of customer personal data can be properly maintained. For this reason, one of the legal efforts that can be given is preventive efforts which are legal efforts to prevent misuse of customer information or data as banking confidentiality data in Islamic banking so that if Bank Syariah Indonesia wants to open customer confidentiality data, Bank Syariah Indonesia is required to request written approval from the customer. In requesting such approval, the bank must first explain the purpose and consequences of providing and/or disseminating customer personal data to other parties outside the bank's legal entity for commercial purposes, unless otherwise stipulated in applicable laws and regulations.

Preventive efforts are not only given to individuals but can also be applied in terms of providing and/or disseminating personal data of bank customers who are legal entities, where the Bank is required to request written approval to disseminate or open personal data of customers to designated customers or the relevant party as a representative of the legal entity. Thus, Islamic banking can carry out its banking business activities based on Islamic principles and statutory provisions.

Bank's Responsibility for Violations of Disclosure of Customer Confidential Data According to Banking Standards at Bank Syariah Indonesia, Pematang Siantar Branch Unit

Bank Syariah is now focusing on integrating BNI Syariah systems and services and BRI Syariah to the Bank Mandiri Syariah system used as BSI's core business. The integration will be carried out to 600 branches of BNI Syariah, BRI Syariah and Bank Mandiri Syariah so that BSI will have 1,365 existing branches and units previously owned by each bank throughout Indonesia, including Bank Syariah Indonesia Pemantangsiantar Branch Unit. In addition to relying on branches, BSI also relies on superior digital banking services through the BSI Mobile application as an omnichannel strategy (a customer-centric approach related to customer experience that can shop on various online shopping channels). Not only that, BSI also focuses on three main banking segments, namely wholesale, retail, and MSMEs in running Islamic banking financing, as well as improving the financial performance of the three banks in the Islamic banking business plan.

The formation of BSI certainly has an impact on consumer or customer service, especially regarding account status, loans, transactions and customer fund deposits from the three Islamic banks. In this merger, BSI maintains Bank Syariah Mandiri's technology which has implemented a core banking database and a branchless banking program formed by BI, so that all bank customer confidentiality data does not need to be converted and has automatically switched to BSI. Meanwhile, BNI Syariah and BRI Syariah customers are encouraged to voluntarily change their accounts independently by online on boarding or registering their accounts at BSI through the BSI mobile banking system and then automatically can changed and at the end (new account) will be sent online or picked up at the nearest BSI branch office or branch unit.

Every transaction and agreement between the customer and the old bank entity also automatically switches to BSI without additional costs, so that the loan or customer relationship at the old bank moves to BSI. Thus, all banking business activities at BSI are

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

subject to Law Number 21 of 2008 concerning Sharia Banking and regulations issued by the Financial Services Authority and Bank Indonesia.

Responsibility is a requirement for someone to carry out what has been required of him, the obligation is in the form of an act related to ethics or morals and causes consequences and consequences in its implementation. Meanwhile, accountability must have a basis, namely something that causes the emergence of legal rights for someone to sue another person as well as something that gives rise to the legal obligation of another person to give accountability to someone.

The results of the researcher's interview with BSI, represented by a resource person named Mr. Septianto Pane as BOSM (Branch Operation and Service Manager), explained that one form of accountability based on Liability without fault in banking is a violation that occurs in opening, providing or selling customer confidential data to third parties without the customer's knowledge, misusing customer confidential data to enrich and benefit oneself or other parties without the customer's knowledge, and misusing the authority, opportunity or means available to him because of his position or position.Therefore, the form of bank accountability that is based on, caused by, and has been proven due to errors or negligence of managers, employees, and third parties working for the interests of BSI as a financial services business actor in the financial services sector will provide compensation to customers or consumers.

The compensation provided can be categorized into 2 (two) forms, namely compensation in the form of immaterial is the provision of compensation whose value cannot be measured or the value of the compensation is determined by the customer by considering the circumstances and losses experienced but can be renegotiated with BSI based on sharia principles until the compensation value is obtained which is equivalent in value, while compensation in the form of material is the provision of compensation whose loss value has been determined so that BSI must provide compensation which is equivalent its value.

Meanwhile, liability without fault known as risk liability or strict liability is a legal act originating from customers who provide their confidential data to third parties through the use of ATM cards at merchants (sellers of goods/services), non-cash payments using debit cards, conducting electronic commerce transactions (e-commerce), as well as the presence of third parties who commit criminal acts in the form of cybercrime, fraud, and customer hypnosis through internet banking, mobile banking, and SMS banking For this reason, the form of accountability given by BSI to customers is in the form of implementing operational risk management, reporting operational risks in banking financial report records, evaluating and forming a more reliable banking information system to support the implementation of customer data and information protection as consumers, implementing a mechanism for handling and resolving customer complaints which are then stated in written form, and reporting the handling and resolution of consumer complaints to the authorities according to the complexity of the problem.

Legal Protection for Customers Based on Financial Services Authority Regulation Number 18/POJK.07/2018 Concerning Consumer Complaints Services in the Financial Services Sector

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Considering that all banking activities can now be done through electronic media such as the internet, the term Internet Banking emerged as a network channel used by customers to open accounts, transfer and make online payments. In carrying out electronic banking (e-banking) activities, banks are required to implement risk management in all banking service activities effectively. Furthermore, the form of legal protection against the disclosure or dissemination of information or data regarding customers can be realized in a consumer complaint service forum in the banking financial services sector.

According to Marulak Pardede, the Indonesian banking system is known for legal protection for depositors which can be carried out in 2 (two) ways, namely:

1. Implicit Legal Protection (Implicit Deposit Protection) is legal protection that comes from bank supervision and guidance to avoid bank bankruptcy. This protection is obtained through:
   a) Legislation;
   b) Protection derived from effective bank supervision and guidance carried out by Bank Indonesia;
   c) Efforts to maintain the continuity of banking business as an institution in particular and protection of the banking system in general;
   d) Maintaining the health level of the bank;
   e) Conducting business in accordance with banking prudential principles;
   f) How to provide credit that does not harm the bank and the interests of customers, and;
   g) Providing risk information to customers.
2. Explicit Legal Protection (Explicit Deposit Protection) is legal protection that comes from the establishment of an institution that functions to guarantee public deposits so that if the bank fails to maintain the health of the bank, the institution will replace the funds or finances that are deposited by the public. in banks as regulated in the Decree of the President of the Republic of Indonesia Number 26 of 1998 concerning Guarantees for General Bank Obligations.

Article 7 of POK Number 18/POJK.07/2018 explains that the complaint acceptance procedure begins with PUJK being required to receive and record every complaint submitted by customers as consumers or representatives of banking consumers made verbally or in writing. Furthermore, PUJK is required to verify to ensure the accuracy of information regarding customers as consumers and submit confirmation of receipt or proof of receipt of the complaint to consumers or representatives of consumers.

Then, PUJK is required to conduct an internal examination of the complaint competently, correctly, objectively, and analyze it to ensure the truth of the complaint within a maximum period of 20 (twenty) working days since the documents directly related to the complaint are received in full. If the consumer complaint causes the consumer to suffer a loss, then PUJK is required to make efforts to resolve the dispute through the courts or outside the courts through the Alternative Dispute Resolution Institution determined by the Financial Services Authority.

INFOKUM
Volume 13, Number 02, 2025, DOI 10.58471/infokum.v13i02
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Then, the bank has implemented several important things in order to provide legal protection for customers, including Legal Protection for customers who use internet banking services and others in terms of technological convenience that has met the aspects of confidentiality, integrity, authentication, availability, access control, and nonrepudiation, implementing User ID and PIN tokens (Personal Identification Number) which always change and can only be used once for each financial transaction carried out, Automatic Log Out which is an automatic termination facility if there is a failure in accessing internet banking, SSL 128-bit encryption is a standard for sending confidential data in the form of secret codes and combinations of key numbers via the internet, and Firewall which is a facility to limit and guarantee that only customers have access to enter the internet banking system.

Then, Legal Protection for privacy policies related to all banking transactions and other account information is carried out by customers being able to notify the relevant bank through the 24-hour call center service available or by directly submitting and submitting a complaint in writing to the relevant bank's CSO.

In this case, the bank will provide compensation in the form of material compensation to the customer according to the losses experienced by the customer if an agreement has been reached between the customer and the bank. This is also proven by the way the bank will first check every transaction instruction from the customer stored in the data center in any form, including tape/cartridge, computer/device printouts, and communications sent electronically between the bank and the customer which are valid evidence, unless the customer can prove otherwise.

CONCLUSION

Conclcusion Of This Paper Are: General Provisions regarding Customer Confidential Data can be described by first explaining the Provisions on Banking Confidential Data Reviewed from Law Number 21 of 2008 concerning Sharia Banking, Customer Information as Banking Confidential Data at Bank Syariah Indonesia Pematang Siantar Branch Unit, and General Provisions regarding Customer Confidential Data according to Banking Standards Reviewed from Law Number 19 of 2016 concerning Information and Electronic Transactions. The obstacles faced by banks in disclosing Customer Confidential Data according to Banking Standards at Bank Syariah Indonesia Pematang Siantar Branch Unit are seen in the fulfillment of the requirements for granting written permission to disclose Customer Confidential Data according to Banking Standards, the implementation of procedures for granting written permission to disclose Customer Confidential Data according to Banking Standards, and internal and external obstacles faced by Bank Syariah Indonesia Pematang Siantar Branch Unit in disclosing Customer Confidential Data. Legal Protection for Customers for Information provided as Confidential Data according to Banking Standards at Bank Syariah Indonesia Pematang Siantar Branch Unit can be in the form of preventive efforts for Customers for Information provided as Confidential Data according to Banking Standards at Bank Syariah Indonesia Pematang Siantar Branch Unit according to Law Number 21 of 2008 concerning Sharia Banking, bank accountability for

violations of disclosing Customer Confidential Data according to Banking Standards at Bank Syariah Indonesia Pematang Siantar Branch Unit, and forms of legal protection for Customers based on Financial Services Authority Regulation Number 18/POJK.07/2018 concerning Consumer Complaints Services in the Financial Services Sector.

REFERENCE

[1] Firly, Nadia, 2018, Create Your Own Android Application. Jakarta
[2] Ghassani, Hishshah, 2016, Penggunaan Algoritma Pencocokan Pola pada Sistem Barcode, Bandung
[3] Ilhami, Mirza, 2017, Pengenalan Google Firebase untuk Hybrid Mobile Apps Berbasis Cordova. Medan
Kejora, Faristya Dara dan Ely Setyo Astuti. Imam Fahrur Rozi, 2016, Kamus Penyakit Hewan Peliharaan dengan Metode Boyer Moore Berbasis Android. Malang
[4] Sovia, Rini, 2010, Model Alternatif Pengganti Teknologi Smartcard untuk Sistem Layanan Absen Ujian. Padang
Subaeki, Beki dan M. Rahmat Jauhari, 2016, Aplikasi Info Halal Menggunakan Barcode Scanner untuk Smartpone Android. Bandung
[5] Astrini, Dwi Ayu, *Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime*, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/7035/6546, diakses pada tgl 26 Juni 2020, pkl 12.00 WIB.
[6] Amina, Zaidatul, *Kajian Pembentukan Otoritas Jasa Keuangan di Indonesia:Melihat dari Pengalaman di Negara Lain*, http://www.google.com/search?q=Kajian+Pembentukan+Otoritas+Jasa+Keuangan+di+Indonesia%3A+Melihat+dari+Pengalaman+di+Negara+Lain&i
[7] Rizki, Mochammad Januar, *Begini Prosedur Peralihan Nasabah Usai Merger 3 Bank Syariah*, Artikel Berita, 10 Februari 2021, https://www.hukumonline.com/berita/baca/lt60239443b8cc5/begini-prosedur-peralihan-nasabah-usai-merger-3-bank-syariah, diakses pada tgl 06 April 2021, pkl 14.00 WIB.
[8] Sjamsuddin, Muhammad Rezza, *Perlindungan Hukum Bagi Nasabah Dalam Bentuk Rahasia Bank*, Jurnal Lex Privatum, Vol. III/No. 4/Okt/2015, hal. 32, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/10068, diakses pada tgl 28 Juni 2020, pkl 16.00 WIB.