E-ISSN : 2963-4946
Vol. 1 No. 09 June 2023
Asian Journal of Social and Humanities
https://ajosh.org/

Legal Responsibilities of Parties Involved in Breaking BRI Accounts Through the WhatsApp Application in the Legal Perspective of Engagement

Imelda Martinelli[1], Pascal Amadeo Yapputro[2], Eriyan Rahmadani Dianova[3]
[1,2,3] Universitas Tarumanagara, Indonesia
Email: imeldam@fh.untar.ac.id, pascal.205210036@stu.untar.ac.id, eriyan.205210009@stu.untar.ac.id

* Correspondence: imeldam@fh.untar.ac.id

KEYWORDS
Banking, Mobile Banking, Law of Engagement, Liability

ABSTRACT
Advances in banking technology are developments in information technology that have had a significant impact on the banking industry. Technological developments have helped banks to improve the efficiency of services and products offered to customers. One of the products of technological advances in banking is Mobile Banking, where customers can make transactions anywhere and anytime. However, this has become a new challenge in the law of engagement related to transactions made by individuals with each other online. This research aims to find out the relationship between account breach through the application with the law of engagement, as well as the responsibility of the parties involved. This research uses normative juridical research method. The conclusion of this research is that there is no banking law on Mobile Banking, the customer is responsible for the imprudence committed against his bank account.

Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)

Introduction

The development of information and communication technology (hereinafter referred to as ICT) reflects the changes that always occur in human society. The Hannover 2011 exhibition in Germany discussed "Industry 4.0" to illustrate how global value chains will revolutionize organizations. By enabling "smart factories", the Fourth Industrial Revolution will create a world where virtual and physical manufacturing systems collaborate flexibly with each other around the world. This allows full customization of the product and the creation of a new operating model. These changes are marked by technological advances in areas such as artificial intelligence, robotics, blockchain, nanotechnology, quantum computing, biotechnology, Internet of Things, 3D printing, and unmanned vehicles (Fonna, 2019).

The development of Technology, Information and Communication (ICT) is a global phenomenon that has changed the world in many aspects. The development of technology, information and communication (ICT) in Indonesia continues to increase from year to year. Based on data released by We Are Social and Meltwater entitled

"Digital 2023", in January 2023, Indonesia's total population is estimated to reach 276.4 million in January 2023, an increase in total 1.8 million from 2022, while internet penetration in Indonesia reaches 77% of the total population, with the number of internet users reaching 212.9 million people. This shows that ICT is increasingly becoming an important part of the daily lives of Indonesians.

The development of information and communication technology (ICT) has had a significant impact on various aspects of life including in the practice of engagement law. Along with technological advancements, business practices and contract transactions are increasingly shifting to the digital realm. This creates new problems in the implementation of engagement law due to the emergence of forms of engagement that previously did not exist in conventional business practices, such as electronic contracts and online payments. Therefore, it is necessary to conduct a legal review of the development of ICT and its influence on the practice of engagement law (Adati, 2018).

Reporting from the OJK page, the need for banking digitalization comes from several factors considering the growth of digital banking in Indonesia considering that the Indonesian economy has a lot of potential to enter the digitalization race. These driving factors are reflected in 3 (three) main areas, namely digital access, digital behavior, and digital trade. Digital opportunities include demographic strength, economic strength and digital financing, access to the internet, and greater business potential. Digital productivity is the ability of devices and the use of mobile apps. Digital commerce includes online commerce (e-commerce), digital banking, and electronic financial transactions (Lestari, 2020).

The types of banking products that take advantage of technological developments include:

1. Automated Teller Machine;
2. Banking Application System;
3. Real-Time Gross Settlement System;
4. Internet Banking; and
5. Electronic Clearing System.

As for the advantages of using technology for banks:

1. Business expansion
   In the past, banks needed to have branches to operate in one location. So it's easy to only have one ATM to be in the area. Then came cell phones, which began to remove the physical barrier that allowed consumers to use their phones for banking. Online banking is now available, which is more convenient as it eliminates space and time.
2. Customer loyalty
   Especially customers who travel a lot will feel comfortable conducting their financial transactions without having to open separate bank accounts in different locations. Can only use one bank.
3. Revenue and cost improvement
   The cost of providing banking services through internet banking can be cheaper than opening a branch or installing an ATM.
4. Competitive advantage
   Banks with Internet Banking will have an advantage over banks without internet banking. In the near future, people are reluctant to open bank accounts that do not have online banking capabilities.
5. New business model

Internet Banking creates a new business model. New banking services can be launched quickly on the web.

In addition to bringing great opportunities to the banking industry, digital transformation also presents challenges that need to be overcome. Other challenges include personal data privacy and data use risks. Examples of common legal disputes related to information security and user privacy. Dealing with transactions at banks easy access through Internet Banking and Mobile Banking They also make transactions easier for other users. But on the other hand, there are security risks such as account fraud or misuse of personal information.

One of the recent Mobile Banking fraud cases was carried out by pretending to be a package courier. Reporting from CNN Indonesia, it was explained that this fraud mode began with fraudsters contacting their victims via WhatsApp. The perpetrator then pretends to be a J&T Express courier trying to verify the identity of the recipient of the package. It also sends an attachment with the file name 'View Package Photo'. In fact, the data extension is not in the usual photo format, such as .jpg or .jpeg, but .apk.

An APK type file is an application that runs on a mobile device. Usually, this type of file is an application that is often not listed in the official application store Play Store or App Store. As a result of negligence in monitoring the file format, the victim clicks on it. This causes the Mobile Banking balance to be claimed to run out. In fact, the victim never runs, opens any applications, or fills in user IDs and passwords on other sites.

In the legal field, the development of ICT also requires regulations that can accommodate various problems that arise. The government and related institutions must be able to anticipate and handle various legal issues related to ICT developments, such as regulations related to data security and user privacy, consumer protection, and regulation of banking transactions through ICT.

The formulation of the problem in this study is 1) Is there an engagement agreement formed between the parties involved in breaking into BRI accounts through the Whatsapp application? 2) How is the legal responsibility of the parties involved in breaking into BRI accounts through the whatsapp application in the perspective of engagement law?

Research methods

The research method used in this study is normative juridical. Normative Juridical is an approach to legal research based on the analysis of applicable legal norms. This research was conducted by reviewing various legal sources such as laws, laws and regulations, court decisions, legal doctrines, and other legal literature. The analysis carried out includes the study of legal principles, legal rules, and legal doctrines and principles that apply in the matter under study. In this study, the author refers to applicable legal aspects to analyze the legal liability of the parties involved in breaking into BRI accounts through the WhatsApp application, including the obligations of banks and customers in maintaining account security.

Results and Discussion

1. Data

Legal liability in the perspective of engagement law in the context of BRI Account breaches through the WhatsApp application has to do with banking data. First, the banking data stolen in the breach came from parties involved in the engagement who are responsible for maintaining the confidentiality of user data, namely banks and technology

platforms. Second, the illegal use of banking data in the breach caused losses to the bank as well as the parties involved in the engagement. Therefore, the parties involved in the engagement have the responsibility to maintain the confidentiality of user data and avoid illegal use of such data. Third, the illegal use of banking data in the breach jeopardizes the security of user data and poses a major risk to banks and technology companies. Therefore, the parties involved in the engagement must comply with the provisions of the engagement and applicable laws in maintaining the confidentiality of user data and saving data security risks (Djamali, 2012).

Data is a collection of information or facts collected, measured, or generated through observation or experiment. Data can be numbers, text, images, audio, or any other form that can be recorded or measured. Data is often considered as raw material for information or knowledge, because the data collected is then processed or analyzed to produce more meaningful information or can be used to make decisions or predictions. Data can be generated from a variety of sources, such as surveys, scientific experiments, records of business transactions, sensor logs, and other sources. In today's digital age, data can be easily stored, accessed, and shared through technologies such as computers and the internet. Data can also be grouped into different types, such as quantitative data (which can be measured in quantities or numbers) and qualitative data (which are related to descriptions and attributes).

Data generally refers to information that has been collected, organized, and processed with the aim of making decisions, solving problems, or developing insights. Data can come in many forms, including text, audio, images, and video, and can be collected in a variety of ways, such as through surveys, experiments, observations, and simulations.

In the context of finance, data refers to information about bank operations, clients, transactions, investments, and other aspects of business. Financial data can be used to analyze trends, identify patterns, and make informed decisions about a bank's operations and strategies. Financial data can include information about bank assets, liabilities, income, expenses, and other financial metrics, as well as data about bank customers, such as demographics, spending habits, and creditworthiness.

Financial data is an important tool for banks to effectively monitor and manage their business, and is often used to:

1. Evaluate the bank's financial performance and identify areas for improvement.
2. Monitor credit and loan risk, and make informed loan decisions.
3. Determine the effectiveness of marketing and advertising strategies.
4. Identify high-potential customers for product and service offerings.
5. Analyze trends in customer behavior and preferences to inform product development and innovation.
6. Analyze transactions to detect and prevent fraud and money laundering.

Overall, financial data is an important resource for banks and other financial institutions, and plays an important role in shaping their business strategies, operational decisions, and overall success (Schwab, 2017).

Banking data refers to a collection of information and transactions related to a bank's operational activities. This data covers various aspects related to customers, accounts, financial transactions, and other activities that occur in the banking environment. Banking data is essential for banks to manage their operations, provide services to customers, as well as for the necessary monitoring, analysis, and reporting.

Here are some examples of banking data commonly collected by banks:

1. Customer Data: Customer personal information such as name, address, telephone number, date of birth, identity number, and other contact information.
2. Account Data: Information about the account opened by the customer, including account number, account type (e.g. savings, current or time deposit), opening date, balance, and transaction history.
3. Financial Transaction Data: Information about financial transactions made by customers, such as fund transfers, cash withdrawals, deposits, bill payments, stock purchases, and other transactions involving the movement of funds.
4. Credit Card Data: Information related to credit cards issued by banks, including card numbers, expiration dates, transaction history, payments, and credit limits.
5. Loan Data: Information about loans provided by banks to customers, including loan type, loan amount, interest rate, term, and other information related to the loan.
6. Security Data: Information related to security measures put in place by the bank, such as user authentication data (e.g. user ID, password, or PIN), login track record, and other security activities.
7. Customer Behavior Data: Information relating to customer behavior and preferences, such as transaction history, spending patterns, product or service preferences, and other activities that may provide insight into the customer.

This banking data is stored and managed with a high level of security and confidentiality, in accordance with applicable legal and regulatory requirements. Banks use this banking data to meet their internal needs, such as risk analysis, product and service development, compliance monitoring, and reporting to regulatory authorities.

Banking data and customer data are included in the category of personal and sensitive data. Therefore, such data should not enter the public domain and should be kept confidential by banks and related parties. In the context of data protection, banking data and customer data are considered as private information. This means that access, use, and dissemination of this data should be limited to only authorized parties, such as banks, related customers, and competent authorities. Banks and financial institutions have legal and ethical obligations to protect the confidentiality of customer data. They should implement appropriate security measures and controls to prevent unauthorized access or misuse of customer data.

In addition, banks must also comply with data privacy regulations set by relevant government and supervisory authorities. For customers, it is important to choose a bank that is trustworthy and that has a good reputation in maintaining the confidentiality of customer data. Customers are also advised to read and understand the privacy policy implemented by the bank, and provide consent or permission only for the use of data in accordance with the specified purpose. However, sometimes there are certain situations where banks or authorities may disclose banking data or customer data to third parties. Examples are when there is an official request from an authorized law enforcement agency in the course of a criminal investigation, or when required by applicable laws or regulations (Sidharta & Kusumaatmaja, 2009).

However, private banking data may become public data for several reasons, including:

1. Data breaches: Banking data held by banks can be leaked or stolen by hackers

who have access to bank systems. This can lead to the leakage of banking data recorded in customer accounts and become public data.

2. Human Error: Banking data recorded in customer accounts can be easily disseminated by humans responsible for maintaining data confidentiality. The person responsible may communicate information inadvertently or inadvertently share data with others.
3. Unethical behavior: There are also people who have access to the bank system who can sell banking data to third parties with profit or bad motives. So, with unethical behavior like this can also cause banking data recorded in customer accounts to become public data.

2. Mobile Banking

Mobile Banking is a service that allows bank customers to perform various financial transactions through mobile devices such as mobile phones or tablets. Mobile banking, often referred to as mobile banking, allows customers to make payments, transfer money, check balances, or perform other transactions using their mobile devices. Mobile banking can help individuals and businesses manage finances more efficiently.

Then to create an online account (in this case BRI) there are several ways that can be done, namely:

1. Through e-form.bri.co.id
   BRI account opening via the internet can be done by accessing the BRI e-form page. On this page, customers can register for opening savings, time deposits, foreign currencies and Customer Fund Accounts (RDN).
2. Through bukarekening.bri.co.id
   In early July 2020, BRI launched a new service, namely account opening through the bukarekening.bri.co.id website. Through this site, BRI customers or prospective customers can open BritAma and BritAmaX savings accounts.
3. Via BRImo App
   This application can be used for account opening, ATM card requests, purchase/top up features as well as credit card payments, installments and tickets are also available.

In the context of the principle of the law of engagement, it can be related to the following sentences:

4. BRI account opening via the internet can be done by accessing the BRI e-form page.
   In the engagement, there is a principle of agreement between the parties involved. In this case, an agreement occurs between the customer who wants to open an account and BRI Bank. Through access to the BRI e-form page, customers and Bank BRI reach an agreement to open an account online.
5. In early July 2020, BRI launched a new service, namely account opening through the bukarekening.bri.co.id website.
   The relevant principle of engagement law is the principle of freedom of contract. In this context, Bank BRI introduced a new service that allows customers or prospective customers to open an account through bukarekening.bri.co.id website. In the principle of freedom of contract, parties have the freedom to determine the terms and conditions of their engagement.
6. This application can be used for account opening, ATM card requests, purchase/top up features as well as credit card payments, installments and tickets

are also available.

The relevant principle of the law of engagement is the principle of consensualism. In this context, the use of the BRImo application to open an account and use various service features shows an agreement between the customer and Bank BRI. Through the use of the application, the parties reach an agreement on the provision of banking services that include account opening, ATM card request, purchase/top up, credit card payment, installments, and tickets.

Overall, these three methods show the existence of legal principles of engagement such as agreements, freedom of contract, and consensualism between customers and Bank BRI in opening accounts online (Muhtarom, 2014).

Mobile Banking security arrangements in Indonesia are regulated by Bank Indonesia through Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Information Technology-Based Financial Services.

Based on Article 8 Paragraph 1 Letter B of Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Information Technology-Based Financial Services, banks must:

"Maintain the confidentiality of consumer data and/or information including transaction data and/or information"

There are aspects of security for electronic communication systems that must provide protection against the following:

1. Alteration, addition or destruction by parties who are not responsible for data and information, both during storage and during the transmission process by the sender to the recipient; and
2. The actions of irresponsible parties who seek to obtain confidential information, whether obtained directly from its storage or when transmitted by the sender to the recipient (eavesdropping attempts).

In this case, the security system of electronic communications must meet the security requirements associated with such parts:

1. Confidentiality
   Confidentiality concerns the confidentiality of data or information, and the protection of information against unauthorized parties.
2. Integrity
   Integrity concerns data protection against attempts to modify the data by irresponsible parties, either as long as the data is stored or as long as the data is transmitted to other parties.
3. Authorization
   Authorization involves monitoring access to certain information. Information stored or transmitted over communication networks shall be available at any time if necessary.
4. Authenticity
   It concerns the ability of a person, organization, or computer to prove the identity of the true owner of the information.
5. Non-Repudiation of Origin
   Non-Repudiability concerns the protection of a party involved in a transaction or communication activity that the back of the party denies that the transaction or activity has actually occurred.
6. Auditability
   The data must be recorded in such a way that against the data all the necessary

confidentiality and integrity requirements have been met, that is, the transmission of the data has been encrypted by the sender and has been described by the recipient accordingly.

Based on the quote above, it can be concluded that the security requirements of M-Banking services must meet several conditions, namely:

1. Mobile Banking applications must be equipped with strong encryption and authentication technologies to protect user data and transactions.
2. Banks should provide detection and prevention systems against suspicious activities, such as unauthorized login activity, suspicious transaction activity, and outside attacks.
3. The Bank shall ensure that the Mobile Banking application can be accessed only by authenticated users and obtain approval from the account owner.
4. The Bank shall guarantee the confidentiality of the user's personal data and prevent the use of such data for unauthorized purposes.

In addition, Bank Indonesia also encourages banks to strengthen security by adopting international standards, such as the Payment Card Industry Data Security Standard (PCI DSS), and developing training and security awareness programs for employees and users.

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard maintained by the PCI Security Standards Council, formed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

However, despite strict regulations for Mobile Banking security arrangements in Indonesia, there are still security risks that may occur due to human factors, such as users not paying attention to security, user inability to understand technology security, or other human errors. Therefore, account owners need to understand the risks and comply with the security rules imposed by banks to protect their accounts from abuse.

In Indonesia, there is no specific regulation regarding Mobile Banking, but there are provisions that can be interpreted and used as a basis and determine the legal protection of customers using Mobile Banking. Some regulations that can be used as the basis for legal protection of Mobile Banking customers, among others:

a. Law Number 10 of 1998 concerning Banking
b. Act No. 23 of 1999 concerning Bank Indonesia as last amended by Law No. 7 of 2009
c. Law Number 36 of 1999 concerning Telecommunications
d. Law Number 8 of 1999 concerning Consumer Protection
e. Law Number 11 of 2008 concerning Electronic Information and Transactions
f. Law Number 3 of 2011 concerning Fund Transfer
g. Bank Indonesia Regulation Number 7/6/PBI/2005 concerning Transparency of Bank Product Information and Use of Customer Personal Data
h. Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in Financial Services Sector
i. Bank Indonesia Regulation No. 18/9/PBI/2016 concerning Payment System Regulation and Supervision and Rupiah Management
j. Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Application of Risk Management in the Use of Information Technology by Commercial Banks

k. Financial Services Authority Regulation Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks
l. Financial Services Authority Regulation Number 18/POJK.07/2018 concerning Consumer Complaint Services in the Financial Services Sector

Alliance

Engagement according to Riduan Syahrani, is a legal relationship between two parties in property, one party (creditor) is entitled to an achievement, the other party (debtor) must fulfill the achievement. Therefore, each connection has "rights" on the one hand and "obligations" on the other. If formulated, an engagement is a legal relationship in the field of property between two more people in which one party is entitled to something and the other party is obliged to something. The legal relationship in this property is a legal effect, a legal effect of a treaty or other legal event that gives rise to an engagement (Dengah, 2015). It can be formulated above, it can be seen that there are 4 (four) elements in the engagement, including:

1. Legal relations; relationships in which the law binds the rights of one party and binds them to another.
2. Wealth; The procedure of legal relations until the legal relationship is declared an obligation.
3. Parties; Legal relations must occur between 2 (two) or more people where there are parties who are entitled to achievements and parties who are obliged to fulfill achievements.
4. Object of law (Achievement); Its characteristics are distinguished into giving something, doing something, or not doing something (article 1234 of the Civil Code).

Anyone can terminate the contract if it meets both subjective and objective requirements established by Article 1320 of the Civil Code. These requirements include:

1. There is agreement from those who make agreements; It is neither an oversight nor a coercion.
2. Ability or ability to be bound by a covenant; The law has stipulated that people who are incompetent in carrying out legal acts are minors (immature) or for those whose age has not reached 21 years and adults who are placed under custody (curatele). A person who is incompetent in performing a legal act or who represents it, by reason of incompetence in performing that legal act, may be asked to refuse a legal act on the grounds that it is illegal or inappropriate.
3. A particular thing (which is the object of the agreement); and
4. Because it is lawful according to the law. The law does not prohibit and does not conflict with public interests and ethics. All agreements made by law or validly are binding (principle of legal certainty)

Based on the arrangement of the two articles above, it can be interpreted that every individual is free to perform the agreement as long as it meets the conditions and can be canceled if there are subjective and objective defects, therefore the agreement has an open system (Setiawan, 2021).

The consequences of making the agreement include the following:

1. The consequences of carrying out an agreement are contained explicitly in article 1338 of the Civil Code states: All agreements made meet the conditions prescribed by law for those who make them (Alle wettiglijk gemaakte

overeenkomsten strekken degenen die dezelve hebben aangenaan tot wet). The purpose of the article is that the party involved in making the agreement, has the rights granted to him by the agreement and is obliged to do the things specified in accordance with the content of the agreement made by the parties.

Meets the requirements in article 1320 of the Civil Code where the makers of the agreement must meet subjective and objective requirements in order to be binding as law for the parties.

2. The principle of freedom of contract, Anson's opinion in English Law reads "the promise, in addition to the declaration of intent, imports the will of the party, which promises that the party will depend on the person entrusted to it." The freedom of contract granted to society by law is to contract for anything. Unless it is contrary to ethics, laws, and public order provisions.
3. The principle of Consensualism, this principle states that covenants and engagements are born from the moment the agreement is reached.
4. The principle of Legal Certainty, this certainty is revealed from the binding force of the agreement as law for the parties.
5. The Principle of Balance, which is the principle that requires both parties to fulfill and execute the agreement. The creditor has the power to demand performance and if necessary can demand repayment of the performance through the debtor's wealth, but the debtor also bears the obligation to execute the agreement in good faith.

Negligence is an act where a perpetrator knows the possibility of adverse consequences for others. To determine the element of negligence is not easy, it is necessary to prove because it is often not promised exactly when a party is required to perform the promised performance (Lukman, 2012).

Prof. R. Subekti SH, argues that default is negligence or negligence which can be in the form of 4 kinds in the form of:

1. Not doing what he has been able to or doing.
   In this situation, the debtor does not realize or has never done his achievements so as to the detriment of creditors / others. In his inability to perform his feat, the debtor must prove that he did not perform his feat because of an event or force majeure (overmacht), because the debtor is also guilty, either, or because of that event.
2. Carry out what he has promised, but not as promised.
   In this case the debtor achieves or achieves his achievements, but it is not perfect.
3. Did as promised but too late.
   In this situation, the creditor is performing or fulfilling his achievements, but it is too late.
4. Do an act that according to the agreement cannot be done.
   In this case the creditor does or does what is prohibited by the agreement.

A breach of engagement is an act that harms one or both parties involved in the engagement. The following actions can be taken in the event of a breach of engagement:

1. Seek Indemnification: The injured party may seek compensation for losses suffered as a result of a breach of engagement. The compensation can be in the form of money or compensation for losses suffered.
2. Termination of Agreement: A party that feels aggrieved by a breach of engagement may terminate the agreement that has been made with the other party, and stop cooperating with that party.

3. Legal Claims: Aggrieved parties can file lawsuits through the courts to resolve disputes arising from violations of engagement.
4. Deliberation Settlement: Sometimes, breach of engagement can be resolved by deliberation between the two parties without involving a third party or legal channel. This is done with the aim of avoiding wasted costs and time to formally resolve disputes (Soenandar et al., 2016).

Formation of the Agreement

In the case of downloading an APK, there is first a process called Authorization. Authorization (permission or consent) is the act of giving the authenticated party permission to do something. Authorization aims to limit actions carried out by unauthorized parties to be able to do something in the information network environment which involves entering data / information, reading data / information, modifying, adding or deleting data / information, exporting or importing data / information, printing data / information.

Furthermore, based on Article 1313 of the Civil Code explains the definition of the agreement that,

"A covenant is an act by which one or more persons bind themselves to one or more others."

From the statement above, it can be drawn that authorization cannot be used as the basis of an agreement because it does not involve an agreement or negotiation between two parties. An agreement based on the elements of an agreement is an agreement made between two parties with the aim of determining the rights and obligations of each party. Agreements involve a process of negotiation and signing between the two parties. Considering the elements of the agreement, it can be concluded that Authorization cannot be used as an agreement because it does not fulfill. Authorization is only the act of giving permission or consent by one party to another without involving negotiation or agreement from both parties.

In the case of account breaches through the application, authorization can occur when the customer gives permission to another person or system to access their account. However, authorization cannot be used as the basis for an agreement between the customer and the application provider, because authorization is only an act of giving permission or approval and does not involve negotiations or agreements between the two parties (Huda, 2020).

Instead, the agreement in this case can be formed through the terms and conditions of use of the application provided by the application provider. These terms and conditions determine the rights and obligations of each party in terms of application use and customer data protection. In the event of any problem or dispute, these terms and conditions may be used as a basis for resolving the dispute.

These terms and conditions are agreements intended to protect intellectual property rights, your responsibility for content, and set guidelines on the use of website information such as cookies.

An engagement born from this kind of concept (terms and conditions) is considered to remain valid and binding on both parties, assuming that if the consumer/partner accepts and is willing to comply with and comply with the terms and conditions determined by the business actor/application service provider, it means that he is voluntarily considered to have agreed and bound himself, even in the context of cyberspace, Signatures from consumers / partners do not need to be affixed, but simply

by clicking / pressing the "Agree" or "Submit" button.

In the case of making an engagement, of course, it is necessary to pay attention to the legal conditions of an agreement contained in Article 1320 of the Civil Code. In the case of BRI customers who download APKs via the Whatsapp application, if there is an agreement to the Terms and Conditions, it is declared null and void because it violates the terms of the cause that is halal according to law.

Obligations of Banks and BRI Customers in Maintaining the Confidentiality of Account Information and Legal Responsibility

The rights and responsibilities of a bank can be detailed as follows:

1. Receive cash and pay documentation that must be paid by customers, such as checks, remittances, bills of exchange and other banking instruments.
2. Pay back the customer's money placed in the bank if requested by the customer.
3. Borrow money from customers.
4. Maintain confidentiality regarding the accounts of customers in relation to bank confidentiality, unless otherwise stipulated by laws and regulations.
5. If the customer has two accounts, there is a moral obligation for the bank to keep the accounts separate from each other.
6. If the account is closed, the bank must have reasonable reasons to close the account.

One of the obligations arising from the relationship between the bank and the customer is the bank's obligation to keep confidential all transactions that occur between the bank and the depository customer. This form of transaction relationship must be kept confidential by the bank to any party except in certain cases, namely:

1. In the framework of coaching and supervision,
2. In the framework of tax purposes,
3. In the framework of judicial interests in criminal cases,
4. In the interests of civil courts between banks and customers,
5. In order to exchange information between banks.

The bank's obligation to protect the security of customer accounts is regulated in various banking and financial regulations in Indonesia, including:

1. Law No. 7 of 1992 concerning Banking (Banking Law) and its derivative regulations. The Banking Law confirms that banks have an obligation to maintain the confidentiality of customer information and protect customer funds held in bank accounts. In addition, banks must also implement adequate security systems to protect customers from security risks.
2. Bank Indonesia Regulation (PBI) No. 12/29/PBI/2010 concerning Electronic Payment System Implementation. This PBI regulates security in the use of electronic banking services, including Mobile Banking. Banks are required to implement certain security standards, such as data encryption, user authentication, and monitoring and detecting suspicious activity.
3. Financial Services Authority (OJK) Regulation No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. This regulation stipulates that banks must provide protection to customers from security risks and must ensure that the banking services provided are safe and reliable.
4. Payment Card Industry Data Security Standard (PCI DSS). This international security standard is used by banks and other financial institutions to keep credit card data and electronic payment transactions safe.

In carrying out its obligations to protect the security of customer accounts, banks must adopt adequate security systems, implement preventive and detection measures against suspicious activities, and provide education and training on banking security to customers and bank employees. Banks must also comply with applicable banking and financial regulations and always keep abreast of the latest technological developments to strengthen the banking security system.

In relation to the responsibility of securing customer money, Indonesia actually has PP No. 34 of 1973 concerning money guarantees at banks. In one dictum it is stated that "in order to achieve the purpose of binding the deposit of funds from the public it is necessary to establish a deposit guarantee of money in the bank." It's just that PP No. 34 of 1973 has not worked until now.

The Banking Law has no provisions that specifically regulate the issue of legal protection of customer deposits. The Banking Law only mentions that bank guidance and supervision are carried out by Bank Indonesia. Theoretically a bank that is otherwise healthy, it seems safe enough to keep funds in that bank. This can be seen from the provisions of Article 37 B of the Banking Law which states:

1. Each bank guarantees public funds deposited with the bank concerned.
2. To guarantee public deposits at banks as referred to in paragraph (1), a deposit guarantee institution was formed.
3. The deposit insurance institution as referred to in paragraph (2) is in the form of an Indonesian legal entity.
4. Provisions regarding the guarantee of public funds and deposit insurance institutions are further regulated by government regulations.

BRI customers' obligations are contained on BRI's website in the Appearance, Announcement, Transfer, Dissemination and Disclosure of Personal Data section which states that "You are responsible for maintaining the confidentiality of Your Personal Data details and must always maintain and be responsible for the security of the device You use to access BRI Services".

The provision used as the legal basis for the use of standard contracts in Indonesia is Article 1338 Paragraph (1) of the Civil Code which stipulates: "all agreements made validly apply as law to those who make them" from the word all can be interpreted that any legal subject can make an agreement with any content, there is freedom of legal subjects to determine the form of agreement. In other words, through the principle of freedom of contract, legal subjects have freedom in making agreements, including opening opportunities for legal subjects to make new agreements that have not been regulated in the Civil Code in order to follow the needs of the community due to the times (Interest agreements).

In terms of Acknowledgment and Agreement regarding the General Privacy Policy for BRI Services, there is a statement stating that

"This Privacy Policy may be amended and/or updated from time to time. BRI advises you to always read carefully and check this page from time to time to find out any changes caused by it.

You may withdraw your consent to any or all collection, use, disclosure of your Personal Data at any time by giving reasonable written notice to the contact listed below.

Depending on the circumstances and nature of the consent You withdraw, You must understand and acknowledge that BRI is authorized to fulfill or not fulfill the request for withdrawal of consent, then You will no longer be able to use the Service. Withdrawal of consent by You may result in termination of Your account or Your contractual

relationship with the relevant BRI, where all rights and obligations owned by each party are still fully protected."

The statement relates to the principle of freedom of contract as it gives users the right to withdraw their consent to the collection, use, and disclosure of Personal Data at any time. However, BRI's decision to comply or not to comply with the request depends on the circumstances and nature of the withdrawn consent, which is part of the negotiation and agreement between the user and BRI. In addition, the statement also confirms that the withdrawal of consent may result in the termination of the user's account or contractual relationship with the relevant BRI, indicating that the contractual relationship is based on freedom and mutual agreement between the two parties.

Based on the statement above, if the BRI customer does not withdraw the statement agreeing to his obligation to be responsible for ensuring the security of the device, then the customer is deemed to have agreed to the obligation and is responsible for the security of the device used to access BRI services. If there is a security breach or unauthorized access to the customer's account caused by the customer's failure to ensure the security of its device, BRI will not be responsible for any losses incurred. Therefore, it is very important for BRI customers to understand and comply with these obligations to avoid unwanted losses.

Based on the obligations that have been described, there is a legal position of the customer and Bank BRI can be determined based on several applicable legal provisions, including:

1. In the event that the customer is negligent in carrying out its obligations in maintaining the confidentiality of the data and electronic information used, the customer can be held responsible for the losses incurred.
2. Based on regulations regarding the bank's obligation to maintain security in general, the responsibility for the security of the customer's personal data lies with the customer himself. However, as a financial service provider, BRI also has the responsibility to maintain and improve its security system to protect customers' personal data from cyber attacks. If BRI is proven to have failed to carry out its duties in maintaining system security, BRI will be responsible for losses caused to customers. However, if negligence occurs due to the customer's fault or negligence, then the responsibility lies with the customer.
3. Article 1365 of the Civil Code regulates legal responsibility for losses caused by a person's fault or negligence. In this case, if the customer or Bank BRI is proven to have committed an error or negligence that resulted in losses, sanctions or compensation claims may be imposed.

BRI itself has provided tips to prevent fraud that will harm customers, including:

1. Never provide data for transactions such as PIN, Username, Password, OTP Code, CVV / CVC Number, ATM Card Number and Expiration Date to anyone.
2. Send SMS, email and telephone on behalf of BRI if asked for PIN, OTP Code, CVV / CVC, ATM Card Number and Expired Date or link provided from unknown parties.
3. Be careful and ignore if you get the OTP code without making any transactions.
4. Never post your date of birth, birth mother's maiden name, ID number, photo ID card, etc. on social media.
5. BRI never updates customer data via SMS or email and BRI-Info is the only promo information media.
6. If you get suspicious activities or links on behalf of BRI, please report to the BRI

contact center 14017/1500017 or callbri@bri.co.id.

Conclusion

Based on the results and discussion as described above, there are several conclusions that can be drawn. In Indonesia, there is no specific regulation regarding Mobile Banking, but there are provisions that can be interpreted and used as a basis and determine the legal protection of customers using Mobile Banking. The rules on Mobile Banking security in Indonesia are regulated by Bank Indonesia through Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Information Technology-Based Financial Services.

Then in the case of downloading an APK, there is a process called Authorization. Authorization (permission or approval) However, the authorization cannot be used as the basis for an agreement between the customer and the application provider, because authorization is only an act of giving permission or approval only and does not involve negotiations or agreements between the two parties. The agreement in this case can be formed through the terms and conditions of use of the application provided by the application provider. Engagements formed from this kind of concept (terms and conditions) are considered to remain valid and binding on both parties. However, it can be null and void because it does not meet the legal conditions of an agreement, namely a lawful clause.

The relevant Bank, namely BRI, explained that, if there is a security breach or unauthorized access to the customer's account caused by the customer's failure to ensure the security of its device, BRI will not be responsible for any losses incurred. Upon BRI's explanation, the customer for his negligence did not ask for compensation against BRI, because the responsibility lies with the customer.

The government and banks can socialize banking rules related to customer account security. In addition, notice of caution in approving third-party applications to access customer personal data such as account pins and mobile banking.

References

Adati, M. A. (2018). Wanprestasi Dalam Perjanjian Yang Dapat Di Pidana Menurut Pasal 378 Kitab Undang-Undang Hukum Pidana. Lex Privatum, 6(4).

AWS. (n.d.). PCI DSS. aws.amazon.com. https://aws.amazon.com/id/compliance/pci-dss-level-1-faqs/

BRI. (2021, 15 April). Kebijakan Privasi dan Pengamanan. Diakses pada 10 Maret 2023, dari https://bri.co.id/privacyDengah, K. (2015). Eksistensi Serta Akibat Penerapan Sistem Terbuka Pada Hukum Perikatan. Lex Privatum, 3(4).

Chandro, B. (n.d.). Apa Itu mBanking? Ini Penjelasan, Fungsi, dan Cara Kerjanya. lifepal.co.id. https://lifepal.co.id/media/banyak-digunakan-orang-sudah-tahu-kelebihan-dan-kekurangan-m-banking-ini/#Fungsi_mBanking.

CNN Indonesia. (2022, December 6). Viral Penipuan Modus Kurir Kirim Foto, Bisa Bobol Data Mobile Banking. www.cnnindonesia.com. https://www.cnnindonesia.com/teknologi/20221206094446-192-883374/viral-penipuan-modus-kurir-kirim-foto-bisa-bobol-data-mobile-banking/amp.

Djamali, R. A. (2012). Pengantar Hukum Indonesia(2 Cetakan). Jakarta: Rajawali Pers.

Fonna, N. (2019). Pengembangan revolusi industri 4.0 dalam berbagai bidang. Guepedia.

Huda, I. A. (2020). Perkembangan teknologi informasi dan komunikasi (TIK) terhadap kualitas pembelajaran di sekolah dasar. Jurnal Pendidikan Dan Konseling (JPDK), 2(1), 121–125.

Kurniawan, Faizal. "Bisakah Syarat dan Ketentuan Aplikasi Disebut Perjanjian?" Hukum Online. 18 Maret 2022. https://www.hukumonline.com/klinik/a/bisakah-syarat-dan-ketentuan-aplikasi-disebut-perjanjian-lt61ef908249fc2.

Lestari, A. P. (2020). Kepastian perlindungan hukum pada klausula baku dalam perjanjian pinjaman online di Indonesia. SUPREMASI: Jurnal Hukum, 2(2), 174–193.

Lukman, S. (2012). Hukum Perjanjian Kontrak,(Panduan Memahami Hukum Perikatan & Penerapan Surat Perjanjian Kontrak) Cakrawala. Yogyakarta.

Microsoft. "Autentikasi vs. otorisasi." 12 Juni 2022. https://learn.microsoft.com/id-id/azure/active-directory/develop/authentication-vs-authorization.

Muhtarom, M. (2014). Asas-asas hukum perjanjian: Suatu landasan dalam pembuatan kontrak.

OJK. (2022, October 13). Transformasi Digital Perbankan: Wujudkan Bank Digital. https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/40774

Schwab, K. (2017). The fourth industrial revolution, Crown Business. New York, 192.

Setiawan, I. K. O. (2021). Hukum perikatan. Bumi Aksara.

Sidharta, B. A., & Kusumaatmaja, M. (2009). Pengantar Ilmu Hukum. Bandung: Alumni.

Soenandar, T., Jamil, F., Badrulzaman, M. D., Sjahdeni, S. R., & Soeprapto, H. (2016). Kompilasi Hukum Perikatan.

Sukirno, S. A. S. A., & Rochmadi, F. (2015). Perkembangan Teknologi Informasi dan Komunikasi. Jurnal Pendidikan Vokasi, 5(1), 43-53.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Wicaksono, Frans Satriyo. Panduan Lengkap Membuat Surat-Surat Kontrak, Hukum Kontrak, Syarat Sah Kontrak, Tahap Prakontrak, Penyusunan Kontrak, Pasca Penandatangan Kontrak. Ciganjur: Visimedia, 2009.

Zyro. "Cara Membuat Syarat dan Ketentuan." https://zyro.com/id/tool/membuat-syarat-dan-ketentuan (diakses pada 10 Maret 2023).