

CONSUMER PROTECTION OF MOBILE BANKING USERS (CASE STUDY OF COMMONWEALTH MOBILE BANKING ACCOUNT BREAKING ON BEHALF OF ILHAM BINTANG)

Muhammad Ilham.

University Of Indonesia

vmuhammadilhamz@gmail.com

Inosentius Samsul

University Of Indonesia

inosentius.samsul@dpr.go.id

Henny Marlyna

University Of Indonesia

hennymarlyna@gmail.com

ABSTRACT

Bank services, in general, are services to store customer funds safely. As one of the bank's primary services, customers can obtain guarantees for funds deposited in the relevant bank. In its development, bank services have used technology assistance to create a mobile banking product. In the case raised in this paper, some customers lose funds at the bank, where the funds are stored use mobile banking. The purpose of this paper is to review the applicable Indonesian laws following the case of Ilham Bintang, a consumer of Commonwealth Bank. This research shall use secondary data from the normative juridical, a process to find the rule of law, legal principles, and legal doctrines to answer the legal issue. The legal topic discussed in this paper is how the applicable laws of banking and consumer protection protect bank consumers specifically, regarding account break-ins. Based on Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking and Law Number 8 of 1999 concerning Consumer Protection, banks as business actors are required to provide compensation, damages, and reimbursement, if offered, are not according to what promise. However, if it proven that this is not the business actor's fault, the business actor may be released from this responsibility.

Keywords: *mobile banking; consumer protection; compensation.*

INTRODUCTION

Banking is one of the most critical driving wheels of the country's economy. The essence of banking is a financial institution that can collect funds from the public and channel them back to the community in the form of credit or other formats. So, the spearhead of the state's economic driver is the bank itself, where only the bank is legally authorized to collect public funds that are considered "excessive" and distribute them directly to other people deemed "needed" it.

The concept of a savings institution for the community applied in 2000 B.C. At that time, an institution called "Temples of Babylon" lent gold and silver with an interest rate of 20% each month.¹ Then from there, the concept of the type of institution that collects public funds

¹Yarsi, *Sejarah Berdirinya Bank di Dunia*, <http://id.yarsi.ac.id/sejarah-berdirinya-bank-di-dunia-4242#:~:text=Sesudah%20zaman%20Babylon%2C%20tahun%20500,muncul%20bankir%20Dbankir%20swasta%20pertama>, accessed on 11 Juni

or wealth (with storage fees) and then channels it back to the community (with interest) continues to be used and developed to this day. Banking is one of the financial institutions oriented to conducting various financial transactions. The most dominant banking transactions include raising funds (funding) and channeling funds (lending). Besides that, other banking transactions support activities to collect and distribute funds.² Banks can function as accepting deposits, distributing credit, receiving credit, distributing financing, investing, creating money, and other services such as a place to store other valuables.³

Banking today has developed a lot compared to the past. Innovations are continuously made to improve customer service and ease of transactions. One of the innovations currently quite busy is internet banking and mobile banking making it easy for customers to complete transactions with their electronic devices anywhere and anytime.

The banking industry innovations are certain intended for convenience and better customer service. Still, in their implementation, this is not free from problems. According to data released by the Financial Services Authority (**OJK**) in the first semester of 2015, there were 644 complaints received by OJK from consumers. Of all these complaints, there were 390 complaints, or 60.5%, originating from banking-related complaints.⁴

One of the banks in Indonesia that provides mobile banking services is PT Bank Commonwealth (“**Commonwealth**”), an Australian bank. However, one of the Commonwealth customers who use mobile banking services, Ilham Bintang, in January 2020 reported that his account had been burglarized and that had lost approximately Rp250 million of funds from his account.

The burglary of Ilham Bintang’s account as a victim of property occurred due to accessing the victim’s Commonwealth mobile banking account. The burglary of Ilham Bintang is made possible by the way the perpetrator controls the SIM card and the victim’s email account, which is the verification stage to access mobile banking using a device other than the victim’s. The procedure for using SIM cards and email accounts to access mobile banking accounts is not only implemented by Commonwealth banks but other banks providing mobile banking services also have the same procedure. Therefore, the case that the case that happened to Ilham Bintang also happened to other customers.

From this case, we can see that mobile banking innovations aimed at facilitating customers also provide opportunities for individuals to take destructive actions. Therefore, the author needs to form an article entitled “Legal Protection of Mobile Banking User Customers (Case Study of Commonwealth Mobile Banking Account Burglary in Ilham Bintang).”

LEGAL ISSUES

The discussion of this paper is intend to enlighten several legal issues raised by Ilham Bintang bank account break-ins as follows:

1. How is the applicable law regulates the bank’s liability in the event of customer loss?
2. How is the legal protection for bank consumers such as Ilham Bintang in case of account break-ins?

2022.

²Trisadini Prasastinah Usanti, *Prinsip kehati-hatian pada Transaksi Perbankan*, (Surabaya: Airlangga University Press. 2013),p. 1.

³Zainal aikin, *Pengantar Hukum Perbankan Indonesia*. (Jakarta: PT.Raja Grafindo Persada, 2015)p. 16.

⁴Nurdin, A. *Kajian Peraturan Perlindungan Konsumen di Sektor Perbankan*. Jurnal Hukum dan Pembangunan 48 No.2, 2018, p. 299-322.

METHODS

The writing method used in this paper is normative research, which is a process of finding the rule of law, legal principles, and legal doctrines to answer the legal problems faced.⁵ It is said to be normative because it is precisely for researching law as a positive norm. Then the normative research method is also a doctrinal research method. This research's nature is prescriptively and aimed at getting suggestions regarding solutions to existing problems. This research also refers to laws and regulations relating to topics and research on library materials or secondary data regarding the issues discussed in this paper. The source and material in this research are primary and secondary materials. The primary material in this research is government laws. Secondary material used in this research is books, journal, news, and other academics writing. This research will mainly connect the applicable laws in banking and consumer protection, especially those related to mobile banking activities, with a case study of breaking into Ilham Bintang's account through a mobile banking account.

ANALYSIS AND DISCUSSION

Regulation Relating to Mobile Banking

The banking function based on Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking ("**Banking Law**") is an intermediary institution in which the Bank acts as a collector and financial intermediary.⁶ This intermediation function will help drive stability and the country's economy.⁷ In this regard, the bank service currently frequently used is mobile banking as a form of improving intermediation services. In principle, now the authorized institution to regulate the implementation of digital banking services is the OJK, where the most recent regulation related to this is controlled through the Financial Services Authority Regulation Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks ("**POJK 12/2018**").

POJK 12/2018 has regulated that if you want to provide Electronic Banking Services, Commercial Banks must apply risk management and prudential principles and comply with the provisions in POJK 12/2018. This precautionary principle is often refer to as the (prudential principal). The word "prudent" literally means "wise" in Indonesian. But in banking, this term is used for "prudence."⁸ Even in the context of banking, other principles must establish, namely the principle of trust (fiduciary relation principle), the focus of prudence (prudential doctrine), the principle of confidentiality (secrecy principle), and the direction of knowing customers (know-how customer principle).⁹

For Electronic Banking Services of a transactional nature, Commercial Banks require to obtain prior will only obtain approval from the OJK. Article 5 of POJK 12/2018 stipulates that will only obtain support from the OJK by applying for license which the following documents must accompany:

- a. Evidence of readiness for the implementation of Electronic Banking Services which at least contains:

⁵Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris*, (Yogyakarta: Pustaka Belajar, 2015), p. 34.

⁶Trisadini P. Usanti dan Abd. Shomad, *Hukum Perbankan*, (Jakarta: Kencana Prenada Media Group, 2016), p. 55.

⁷Rani Apriani dan Hartanto, *Hukum Perbankan dan Surat Berharga*, (Yogyakarta: deepublish, 2019), p 1.

⁸Trisadini P. Usanti dan Abd. Shomad, *Hukum Perbankan*, (Jakarta: Kencana Prenada Media Group, 2016), p 122.

⁹Neni Sri Imaniyati dan Panji Adam Agus Putra. *Pengantar Hukum Perbankan Indonesia*. (Bandung: Sinar Grafika, 2016), p. 18.

1. a supportive organizational structure, including supervision from the management;
 2. policies, systems, procedures, and authorities in the issuance of Electronic Banking Services products;
 3. readiness of Information Technology infrastructure to support Electronic Banking Service products;
 4. results of analysis and identification of risks inherent in Electronic Banking Service products;
 5. readiness to implement risk management, especially security control, to ensure the fulfillment of the principles of confidentiality, integrity, authentication, non-repudiation, and availability;
 6. the results of the analysis of legal aspects;
 7. description of an accounting information system; and
 8. customer protection and education programs;
- b. The results of the business analysis regarding the projection of new Electronic Banking Services products issued in the next 1 year period; and
- c. Other supporting documents if required.

In addition to these documents, Commercial Banks are also required to provide inspection results from independent parties to provide opinions on product characteristics and the adequacy of Information Technology system security related to products as well as compliance with the provisions of laws and regulations in Indonesia, and practices or standards that apply nationally and internationally. Where must apply for approval to the OJK by two months before implementation of the service?. Of course, the requirements as regulated in POJK 12/2018 do not reduce the obligation of Commercial Banks to comply with other commitments held in other laws and regulations.

Furthermore, based on Article 6 of POJK 12/2018, service provider banks are required to apply the principle of controlling data security and customer transactions from Electronic Banking Services on each electronic system, including, among others:

- a. confidentiality;
- b. integrity;
- c. availability;
- d. authentication;
- e. non-repudiation;
- f. authorization of control;
- g. segregation of duties, and
- h. maintenance of audit trails.

POJK 12/2018 has also anticipated security standards rather than business relationships between the Bank and customers or prospective customers in Digital Banking Services. In Article 11 of POJK 12/2018, banks must identify and verify documents from these customers or potential customers. The verification can also be done face-to-face or without using software provided by the Bank with hardware owned by the Bank or customers or prospective customers. In this process, the Bank is required to perform at least 2-factor authentication (two-factor authentication). The following are the types of authenticity factors as stipulated in the Elucidation of Article 11 paragraph (3) of POJK 12/2018:

- a. what you know
including Personal Identification Number (PIN), password, identity card number, and personal data.
- b. what you have (what you have)
including magnetic cards, chip cards, tokens, digital signatures, and other equivalent forms
- c. your characteristics (what you are)

including biometrics such as fingerprints, voice, and iris

If the verification process is not carry out face-to-face, one of the authenticity factors must be your hallmark (what you are).

Bank Accountability

Based on the Banking Law, banks provide their customers three types of legal protection.¹⁰ They are, first providing information regarding the possible risk of loss. This is regulate in Article 29, paragraph (4) of the Banking Law, which essentially states that banks must provide information if there is a potential risk of loss in terms of customer transactions through banks. This provision aims to ensure transparency in the banking world.

Second is the confidentiality guarantee as regulated in Article 1 number 28 jo, Article 40 paragraphs (1) and (2) of the Banking Law. Please note that this bank secrecy guarantee applies only to customers who deposit or have deposits at the bank, so it does not apply to customers who borrow money from the bank. This confidentiality guarantee is one reason people can trust banks to keep their funds. Of course, this confidentiality guarantee also has its exceptions as regulated in the Banking Law and other laws and regulations.

The third is a guarantee for customer funds deposited in banks through the Deposit Insurance Corporation (“LPS”). Article 37B paragraphs (1) and (2) of the Banking Law oblige every bank to guarantee the funds of customers who deposit money in the bank. From this article then, the LPS was formed as a legal entity that would provide guarantees for customer deposits.

In addition the Banking Law, relationship between customers and banks also include the relationship between consumers and business actors. Banking law follow Article 1 points 16 and 17, which together can be conclude that a customer can be a depositor who keeps his funds in a bank based on a bank agreement with the customer concerned. In this way, banks must also comply with Law Number 8 of 1999 concerning Consumer Protection (“**Consumer Protection Law**”).

Article 7 letter g of the Consumer Protection Law allows banks as business actors to provide compensation, compensation, and reimbursement if the services offered to consumers are not following the agreement. In this case, the services offered to consumers are depositing customer funds in banks. This provision is also regulated by Article 19, paragraphs (1) and (2), which essentially states that if a customer as a consumer suffers a loss due to the use of bank services, the bank must be responsible for providing compensation which can be in the form of a refund or replacement of goods and goods. Services of the same type or equivalent in value, or health care and compensation following the provisions of the applicable laws and regulations. However, Article 19 paragraph (5) also stipulates that business actors are free to provide compensation if the business actor can prove that the error is the fault of non-bank consumers.¹¹

Consumer Protection in Cases of Mobile Banking Account Break-ins

Ilham Bintang’s case began with a suspect named Desar, who had illegally purchased Ilham Bintang’s personal data from Hendrik as an employee at the BPR Bintara Pratama Sejahtera bank. After getting Ilham Bintang’s data, the perpetrator tried to contact Ilham Bintang using a phone number that had purchased illegally before. When Desar attempted to call the number it was not active because Ilham Bintang was on his way to Australia. On that basis, Desar took

¹⁰Abi Jam’an Kurnia, *Bentuk-Bentuk Perlindungan Hukum oleh Bank kepada Nasabah*, https://www.hukumonline.com/klinik/detail/ulasan/lt57a4a938b313e/bentuk-bentuk-perlindungan-hukum-oleh-bank-kepada-nasabah/#_ftn2, accessed on 15 June 2022.

¹¹Bernadetha Aurelia Oktavira, *Tanggung Jawab Bank atas Pembobolan Rekening Nasabah* https://www.hukumonline.com/klinik/detail/ulasan/lt5ea6e27adf366/tanggung-jawab-bank-atas-pembobolan-rekening-nasabah/#_ftnref6, accessed on 13 June 2022.

the opportunity to form a fake Identity Card (“KTP”) using Ilham Bintang’s data, which used to duplicate Ilham Bintang’s SIM card at one of the Indosat Ooredoo outlets (telecommunication service provider). Next, Desar hacked into Ilham Bintang’s email account to find out the password for Ilham Bintang’s Commonwealth mobile banking account. With SIM card mastery, Desar only needs to verify the One Time Password (“OTP”) to enter Commonwealth mobile banking with the Desar device and transfer funds to a holding account that has also been prepared previously.

Ilham Bintang as a victim, felt that something was wrong on January 4, 2020. At the time, in Australia, the SIM card could not be used even though the roaming feature to use a SIM card abroad had been activated previously. On January 6, 2020, when Ilham Bintang failed to log into Commonwealth’s mobile banking account, he contacted the Commonwealth agency and received news that his stored funds had been depleted. At this time, the authorities have arrested Desar as well as seven other suspects who are suspected of having helped in the case. 8 suspects, including Desar, are currently being legally processed on suspicion of violating Article 35 in conjunction with Article 51 Paragraph 1 in conjunction with Article 30 in conjunction with Article 46 Paragraph 1 of Law Number 11 of 2008 concerning ITE and Article 363 of the Criminal Code, Article 263 of the Criminal Code, Article 3 and 4 in conjunction with Article 10 of the Republic of Indonesia Law number 8 of 2010 concerning the prevention and eradication of money laundering.¹²

In the case of loss suffered by Ilham Bintang, as a depositor of the Commonwealth bank, there was a loss because his savings had been used by someone else. In this case, it will be discussed first whether there was an error from the consumer or the Commonwealth bank as a business actor based on the existing facts.

From Ilham Bintang’s point of view, customers only need to use bank services as provided for them. Ilham Bintang has also never divulged his data, especially those related to deposits, such as passwords, Time Passwords, or other security facilities, to the perpetrators. It is known from the chronology of the case that there was indeed a provision of customer data to one of the BPR banks, but this was a common thing to do if Ilham Bintang also wanted to become a customer of the relevant BPR bank.

Commonwealth Bank as a provider of fund storage services in the form of a bank, also provides mobile banking services, which are included in the digital banking service category, to its customers, including Ilham Bintang. Ilham Bintang suffered losses of up to hundreds of millions of rupiah through this mobile banking break-in. As one of the banks that provide mobile banking services, it must implement security standards set out in POJK 12/2018.

In POJK 12/2018, it is stipulated that in conducting business relationships through digital banking services, banks must identify customers or prospective customers and verify the information and supporting documents for customers or prospective customers. As explained above, verification can be done face-to-face, or without face-to-face where both can use the Bank’s software with the Bank’s hardware or the customer’s or prospective customer’s hardware.

Furthermore, Article 11 paragraph (3), (4), and (5) also stipulate that in the verification process, banks must apply at least two-factor authentication. This authenticity factor consists of 3 kinds, namely:

- a. what you know

¹²Jimmy Ramadhan Azhari, *Kronologi Ilham Bintang Kehilangan Ratusan Juta Rupiah Akibat Pembobolan Rekening*, <https://megapolitan.kompas.com/read/2020/07/08/18275931/kronologi-ilham-bintang-kehilangan-ratusan-juta-rupiah-akibat-pembobolan?page=all>, accessed on 10 June 2022.

including Personal Identification Number (PIN), password, identity card number, and personal data.

b. what you have (what you have)

including magnetic cards, chip cards, tokens, digital signatures, and other equivalent forms

c. your characteristics (what you are)

including biometrics such as fingerprints, voice, and iris

Verification without face-to-face must apply your distinguishing factor (what you are) as one of the authenticity factors. In the case experienced by Ilham Bintang, explained that the mobile banking burglary was carried out by the perpetrator using his hardware without any face-to-face verification. From this arises the bank's obligation to apply your distinguishing factor (what you are) as one of the authenticity factors when authorizing. This authenticity factor is not used by Commonwealth banks when the perpetrators try to access Ilham Bintang's mobile banking and transfer funds.

CONCLUSION

Based on the above discussion, the writer then has several conclusions answering the legal issue raised in this writing:

1. Banks can provide mobile banking services to their customers as a form of digital banking services. OJK has also issued POJK 12/2018, which regulates explicitly the Implementation of Digital Banking by Commercial Banks. In POJK 12/2018, banks must meet security standards as a form of consumer protection in the financial services sector. This security standard has a customer or prospective customer identification and verification process. In this verification process, the bank must be able to apply at least two authenticity factors. If the verification is not done face-to-face, the authenticity factor used is one of your characteristics (what you are).

The Banking Law provides three types of protection to customers. First, the customer has the right to be given the risk of customer transactions made through the bank. Second, the bank must keep information on customers who deposit funds confidential. Third, every bank is obliged to guarantee customer funds are stored in the bank. The Consumer Protection Law also applies to the relationship between customers and banks. Business actors are obliged to provide compensation, compensation, and reimbursement if the services offered are not following what was agreed upon where this is regulated in the Consumer Protection Law. However, the Consumer Protection Law waives the responsibility of business actors if be proven that the error is not the fault of the business actor.

2. Ilham Bintang and the Commonwealth bank are the depositor's relationship with the bank or the relationship between consumers and business actors. Therefore, the Consumer Protection Law also applies in discussing related cases. Article 19 of the Consumer Protection Law stipulates that banks as business actors are required to provide compensation for losses suffered by Ilham Bintang as a consumer. However, this obligation will become invalid if the bank can prove that the failure was caused by the consumer's fault, not the business actor's fault. In this case, Ilham Bintang has fulfilled its obligations as a customer by not providing personal data to unauthorized parties, especially those related to banking. The Commonwealth Bank has also implemented on duty to apply the authenticity factor. It's just that the application of the authenticity factor is not appropriate because in conducting customer verification or non-face-to-face prospective customers, you are required to apply your characteristic

fairness factor (what you are) as one of the authenticity factors that will be used. Applying your distinguishing fairness factor (what you are) will most likely prevent the risk of a mobile banking break-in, as experienced by Ilham Bintang, because it uses customer biometrics. In this case, the author assumes that the error occurred with the Commonwealth bank because it did not apply the appropriate authenticity factor and, therefore must be responsible for Ilham Bintang's losses.

BIBLIOGRAPHY

Books

- Alkin, Zainal, (2015), *Pengantar Hukum Perbankan Indonesia*, PT.Raja Grafindo Persada, Jakarta
- Apriani, Riani dan Hartanto, (2019), *Hukum Perbankan dan Surat Berharga*, deepublish, Yogyakarta
- Imaniyati, Sri Neni dan Panji Adam Agus Putra, (2016), *Pengantar Hukum Perbankan Indonesia*. Sinar Grafika, Bandung
- ND, Mukti Fajar dan Yulianto Achmad. *Dualisme Penelitian Hukum Normatif dan Empiris*, (2015), Yogyakarta: Pustaka Belajar.
- Usanti, Trisadini P., (2013), *Prinsip Kehati-hatian Dalam Hukum Perbankan*, Airlangga University Press, Surabaya.
- Usanti, Trisadini P. dan Abd,Shomad, (2016), *Hukum Perbankan*, Kencana Prenada Media Group, Jakarta

Journal

- A., Nurnid, (2018), *Kajian Peraturan Perlindungan Konsumen di Sektor Perbankan*. Jurnal Hukum dan Pembangunan 48 No.2,

News and Article

- Azhari, Jimmy Ramadhan, *Kronologi Ilham Bintang Kehilangan Ratusan Juta Rupiah Akibat Pembobolan Rekening*, (<https://megapolitan.kompas.com/read/2020/07/08/18275931/kronologi-ilham-bintang-kehilangan-ratusan-juta-rupiah-akibat-pembobolan?page=all>),
- Kurnia, Abi Jam'an, *Bentuk-Bentuk Perlindungan Hukum oleh Bank kepada Nasabah*, (https://www.hukumonline.com/klinik/detail/ulasan/lt57a4a938b313e/bentuk-bentuk-perlindungan-hukum-oleh-bank-kepada-nasabah#_ftn2),
- Bernadetha Aurelia Oktavira, *Tanggung Jawab Bank atas Pembobolan Rekening Nasabah* (https://www.hukumonline.com/klinik/detail/ulasan/lt5ea6e27adf366/tanggung-jawab-bank-atas-pembobolan-rekening-nasabah/#_ftnref6)
- Yarsi, *Sejarah Berdirinya Bank di Dunia*, (<http://id.yarsi.ac.id/sejarah-berdirinya-bank-di-dunia-4242#:~:text=Sesudah%20zaman%20Babylon%2C%20tahun%20500,muncul%20bankir%2Dbankir%20swasta%20pertama>),

Regulations

Indonesia, Law Number 10 of 1998 concerning Amendments of Law Number 7 of 1992 concerning Banking, Republic of Indonesia State Gazette of 1998 Number 182, and Supplement to the State Gazette 3790.

Indonesia, Law Number 8 of 1999 concerning Consumer Protection, Lembaran Negara Republic of Indonesia State Gazette of 1999 Number 22, and Supplement to the State Gazette 3821.

Indonesia, Financial Service Authority Regulation Number 12/POJK.03/2018 tentang Digital Banking Service of Banks, Republic of Indonesia State Gazette of 2018 Number 127, dan Supplement to the State Gazette 6235.