

Bank Responsibility on Customer's Data Fraud in Indonesia



Andrian¹, Bambang Eko Turisno²

^{1,2}Fakultas Hukum, Universitas Diponegoro, Jl. Prof. Soedarto, SH. Tembalang, Semarang, 50275

ABSTRACT: Banks as financial institutions certainly have a very important role in a country, especially to advance the economy in that country. So, the good running of the banking industry in one country is a very crucial thing to be regulated by the state. With the presence of technology, the threat of cybercrime is now a serious concern, especially in the banking world, especially with regard to the confidentiality of customer data. This study uses a normative juridical method. Based on the existing regulations, it can be concluded that it is crucial for banks to continue to improve security, especially with regard to customer data and the Bank must be responsible for losses that occur if the data leak is caused by the bank's negligence in building a security system.

KEYWORDS: Bank, Responsibility, Customer data.

A. INTRODUCTION

The era of globalization has changed the world order that is increasingly borderless (borderless) and increases the interconnectedness between communities whose interconnectedness is shown from the influence between humans living in other parts of the earth (Baylis and Smith, 2001). Of course, this has a positive impact in terms of making it easier for people to access information that is useful for building insights that are now not only local, but interlocal.

One factor closely related to globalization and the times is the development of technology and information. The rapid development of information technology has changed human life to be easier by making everything effective and efficient not only for certain circles but covering the entire community including government and private agencies (Sidik, 2013). Since 1960, when the first computer business was established for the public, at that time information technology has changed the way trade is carried out throughout the world (Awad, 2003). It is undeniable that the progress of the times and science and technology are things that will go hand in hand and influence each other and have an impact on various aspects of life, especially on people's attitudes in responding to these advances and influencing the pattern of people's lives (Andi Hamzah, 2000).

On the one hand, the presence of globalization and technology-based community activities certainly has a positive impact in terms of making it easier for people to access information that is useful for building their insights which are now not only local, but interlocal. But on the other hand, globalization certainly has a negative impact on society, which is shown by the emergence of cultural and social problems where there has been a westernization of the Indonesian state (Lombard, 2005), as well as through the presence of science and technology-based crimes or what is often referred to as cybercrime. It cannot be denied that the ease of public access to the internet in this modern era has an impact on the easy use of the internet to commit crimes, which is further exacerbated by one of the characteristics of the globalization era, namely the existence of borderless interactions so that data passing through cyberspace is generally open and uncontrollable (Hafidz, 2014). As it is said that crime is a product of society itself, which means that the level of human civilization is also the driving force of the increasingly sophisticated modes of crime that occur today (Suardi, 2011). The form of cybercrime itself varies. In general, it can be in the form of spreading hoaxes, violent videos, pornography, material about illegal drugs, computer viruses and malware which in addition to damaging the victim's system/network also has the potential to hack and steal data through cyberspace (Abdulhamid, et.al., 2013).

With the presence of technology that facilitates human activities, the threat of cybercrime is now a serious concern, especially in the banking world. The existence of advances in science and technology clearly threatens the existence of the banking industry, especially with regard to the confidentiality of customer data. Customer data is the most crucial thing in the banking business where data leakage can potentially cause financial losses experienced by customers. For example, currently there is a rampant credit card breach experienced by customers where the fraudster can find out customer data such as name, address, telephone number and even the card number owned by the customer even though the customer feels that he has never shared the data with anyone. Of course this then becomes a question, how safe is the bank's protection of customer data, and if problems like this occur, how is the responsibility held by banks, especially according to the Law of the Republic of Indonesia 7 of 1992 jo. Law

Bank Responsibility on Customer's Data Fraud in Indonesia

Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking (Banking Law) and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law).

B. RESEARCH METODE

This research uses a normative juridical method, which uses an approach that refers to primary legal materials in the form of related laws and regulations (Soemitro, 1982), while the normative approach is carried out by examining library materials on legal principles and case studies so that it is often referred to as library legal research (Mamudji, 2004).

Normative legal research uses secondary data sources and in this research the law is conceptualized based on the doctrine adopted by the conceptualizer using a statutory approach (Shidarta, 2013). The normative juridical method in this paper will analyze primary legal materials in the form of all regulations and laws related to banks, customer protection, and the ITE Law.

C. RESULTS

Banks as financial institutions certainly have a very important role in a country, especially to advance the economy in that country (Sulistyo, 2017). This can be seen from the contribution of consumption and investment activities in the banking world which contributes 80% to the national economy (Hutauruk, 2020). This influence further shows how the position of banks as intermediary institutions cannot be separated anymore in people's lives (Zulfi Diane Zaini, 2014). Seeing the importance of the existence of this bank, the good running of the banking industry in one country is a very crucial thing to be regulated by the state.

The position of the bank is as a financial intermediary, which functions to collect and distribute public funds and also to provide services in payment traffic (Djumhana, 2012). This function then makes the bank obliged to maintain any infrastructure owned and used in payment traffic, including in this case maintaining the confidentiality of customer data.

Regarding the obligation to maintain data confidentiality itself is regulated in Article 40 of the Banking Law which states:

"(1) Banks are obliged to keep information about Depositing Customers and their deposits confidential, except in the cases referred to in Article 41, Article 41A, Article 42, Article 44, and Article 44A. (2) The provisions referred to in paragraph (1) shall also apply to Affiliated Parties."

Furthermore, this exception can be made with conditions, among others. First, for tax purposes as stipulated in Article 41 paragraph (1) that:

"For the purpose of taxation, the Chairman of Bank Indonesia at the request of the Minister of Finance is authorized to issue a written order to the bank to provide information and show written evidence and letters regarding the financial condition of certain depositing customers to tax officials."

Second, relating to the settlement of bank receivables which is regulated in Article 41A that:

"(1) For the settlement of bank receivables that have been handed over to the State Receivables and Auction Agency / State Receivables Affairs Committee, the Chairman of Bank Indonesia gives permission to officials of the State Receivables and Auction Agency / State Receivables Affairs Committee to obtain information from banks regarding deposits of Debtor Customers.

(2) The permission as referred to in paragraph (1) shall be granted in writing upon written request from the Head of the State Receivables and Auction Agency/Chairman of the State Receivables Affairs Committee.

(3) The request as referred to in paragraph (2) shall state the name and position of the official of the State Receivables and Auction Affairs Agency/Committee for State Receivables Affairs, the name of the Debtor Customer concerned."

Third, in the interest of criminal justice. This is regulated in Article 42, namely:

"In the interest of justice in criminal cases, the Chairman of Bank Indonesia may grant permission to the police, prosecutors, or judges to obtain information from banks regarding the deposits of suspects or defendants in banks. Banks are obliged to provide information as referred to in Article 41, Article 41A, and Article 42."

Fourth, there is a need in civil cases between banks and customers in Article 44, namely:

"In a civil case between a bank and its customer, the board of directors of the bank concerned may inform the court about the financial condition of the customer concerned and provide other information relevant to the case."

And fifth, if there is a request for the consent or authorization of the customer in Article 44A:

"(1) Upon request, consent or power of attorney from a depositing customer made in writing, the bank shall be obliged to provide information about the depositing customer's savings at the bank concerned to the party appointed by the depositing customer.

(2) In the event that the Depositor Customer has passed away, the legal heirs of the Depositor Customer concerned are entitled to obtain information regarding the Depositor Customer's deposits."

That is, except for these five reasons, the confidentiality of data from bank customers is a responsibility imposed on the Bank. Indeed, if there is a breach of customer data, especially by using technology such as by hacking, cracking, or manipulation of data, the Banking Law has regulated criminal threats, namely in Article 47 of the Banking Law (Talumewo, 2013). But in order to maintain bank confidentiality, the Banking Law also regulates strict sanctions for members of the board of directors, board of

Bank Responsibility on Customer's Data Fraud in Indonesia

commissioners, bank employees and related parties related to the confidentiality of customer data in Article 47 paragraph (2), namely:

"Members of the Board of Commissioners, Board of Directors, bank employees or other Affiliated Parties who deliberately provide information that must be kept confidential according to Article 40, shall be punished with imprisonment of at least 2 (two) years and a fine of at least Rp 4,000,000,000.00 (four billion rupiah) and a maximum of Rp 8,000,000,000.00 (eight billion rupiah)."

Thus, the bank also protects customer funds in the payment system, where the bank's obligation in order to protect customer rights as consumers has been regulated in Article 1 paragraph (2) and paragraph (3) of Bank Indonesia Regulation Number 16/1/PBI/2014 concerning Consumer Protection of Payment System Services that:

"(2) Payment System Services Consumer Protection, hereinafter referred to as Consumer Protection, is all efforts that ensure legal certainty to provide protection to Payment System Services Consumers.

(3) Payment System Services Consumer, hereinafter referred to as Consumer, is any individual party that utilizes Payment System services from the Provider for their own benefit and not for trade."

The confidentiality of customer data protected by the bank also includes in the event that the customer uses facilities provided by the Bank as a means of electronic transactions and payments regulated in Article 2 of PBI No.16/1/PBI/2014, which states:

"Consumer Protection regulated in this Bank Indonesia Regulation covers Consumer Protection in Payment System service activities which include:

- a. Issuance of fund transfer and/or fund withdrawal instruments.
- b. Fund transfer activities.
- c. Card payment instrument activities.
- d. electronic money activities.
- e. Activities of providing and/or depositing Rupiah money; and
- f. Implementation of other Payment Systems that will be stipulated in Bank Indonesia regulations."

So, with reference to this provision, it is an obligation for banks to monitor every matter relating to customer activities in using banking services including the confidentiality of customer data and losses incurred due to bank negligence in maintaining customer data are part of the Bank's responsibility. This is based on the regulation in Article 1367 of the Civil Code, namely:

"A person is not only responsible for losses caused by his own actions, but also for losses caused by the actions of those who are his dependents or by goods under his supervision".

In practice, liability for the loss of customer money due to bank negligence in safeguarding customer data, for example, in the case of skimming at ATMs. This liability can be seen from the actions of banks to compensate customers for the loss of customer money. For example, in the case of skimming experienced by BRI customers in Cianjur Regency, BRI Bank investigated the case and if the loss of customer funds was indeed caused by skimming, BRI would compensate the customer for the loss within a maximum of 20 working days after the customer's report was received (Yun, 2021).

Other customer data leaks can occur, for example in the case of credit card breaches where there are transactions that are charged to the customer while the customer feels that he did not make the transaction. Regarding problems like this, banks such as BCA Bank are obliged to follow up on reports made by customers by tracing whether it is true that the transaction was not made by the customer. If the transaction is found not to have been made by the customer, then the transaction cannot be billed to the customer. However, problems like this are complaints, or can only be processed if there are complaints from customers about transactions that are not carried out. So customer awareness of data security is needed to avoid losses like this.

Other problems related to customer data leakage can also be caused by customer unrest over offers of products provided by banks such as insurance and others. This is certainly a big question for customers, regarding how these parties know their data. This was revealed from the rise of public complaints that were disturbed by certain parties offering credit card products, insurance, or other products by telephone even though the customer felt that he had never given the phone number to the caller, and it turned out that the caller claimed to be a telemarketing employee of a company that obtained bank customer data from the suspect (Permata, 2018).

A real case of this was found in a study in Bali with the following explanation:

"a. The ANZ Bank has informed the name and cellphone number data to the customer (I Dewa Gede Wirasatya Purnama), which the ANZ bank informed the customer's data to the leasing company in order to offer credit services to the customer and after being traced by the customer it turns out that the leasing company got the customer's data from the ANZ bank. From this it can be seen that ANZ bank has violated the obligation to the confidentiality of bank data. (based on interview dated October 1, 2015)

b. BCA Bank has provided the data of a customer (Nyoman Riela Pricilia) to a third party in the form of an insurance company without the knowledge of the customer in order to offer insurance services. (based on interview dated November 1, 2015)

c. Bank Cimb Niaga has provided data from a customer (Putu Mas Siki Hemalini) in the form of telephone number data to the insurance company as well as experienced by the customer point b above. (based on interview dated November 3, 2015)"

Bank Responsibility on Customer's Data Fraud in Indonesia

This certainly needs to be a serious concern because the three cases show the awareness of the Bank to leak customer data. Apart from the Banking Law, from the point of view of the ITE Law, data leaking is also a wrong thing for banks to do, which is regulated in Article 26 of the ITE Law which states:

"(1) The use of any information through electronic media concerning a person's personal data must be done with the consent of the person concerned.

2) Any person whose rights are violated as referred to in paragraph (1) may file a lawsuit for losses incurred under this Law."

In addition, the obligation to maintain data confidentiality is also regulated in the Financial Services Authority Regulation (POJK) Number 1 / POJK.07 / 2013 concerning Consumer Protection in the Financial Services Sector, which in Article 31 says:

"(1) Financial Services Business Actors are prohibited in any way, from providing data and / or information about their Consumers to third parties.

(2) The prohibition as referred to in paragraph (1) shall be excluded in the event that: a. the Consumer provides written consent; and/or b. required by laws and regulations.

(3) In the event that a Financial Services Business Actor obtains personal data and/or information of a person and/or group of persons from another party and the Financial Services Business Actor will use the data and/or information to carry out its activities, the Financial Services Business Actor must have a written statement that the other party has obtained written consent from the person and/or group of persons to provide the personal data and/or information to any party, including the Financial Services Business Actor.

(4) Cancellation or partial change of consent to the disclosure of data and or information as referred to in paragraph (2) letter a shall be made in writing by the Consumer in the form of a statement letter."

In addition, bank liability for consumer losses is also regulated in Article 29 which states:

"Financial Services Business Actors shall be liable for Consumer losses arising from errors and/or omissions, management, employees of Financial Services Business Actors and/or third parties working for the benefit of Financial Services Business Actors."

Thus, based on these regulations, it is crucial for banks to continue to improve security, especially with regard to customer data and the Bank must be responsible for losses incurred if the data leakage is caused by the bank's negligence in building a security system. Both when data leakage is carried out by other parties such as hackers and when the leakage is carried out by the bank, for example to the insurance company, the bank must still be subject to both criminal and civil liability.

D. CONCLUSION

The confidentiality of data from bank customers is a responsibility imposed on the Bank. It is an obligation for banks to monitor every matter relating to customer activities in using banking services including the confidentiality of customer data and losses incurred due to bank negligence in maintaining customer data is part of the Bank's responsibility. Thus, based on these regulations, it is crucial for banks to continue to improve security, especially related to customer data and the Bank must be responsible for losses incurred if the data leakage is caused by the bank's negligence in building a security system. Both when data leakage is carried out by other parties such as hackers and when the leakage is carried out by the bank, for example to the insurance company, the bank must still be subject to both criminal and civil liability.

REFERENCES

- 1) ABDULHAMID, S. M., and IBRAHIM, F. F. (2013). Controlling Citizen's Cyber Viewing Using Enhanced Internet Content Filters. *International Journal of Information Technology and Computer Science*.
<https://doi.org/10.5815/ijitcs.2013.12.07>
- 2) Andi Hamzah. (2000). *Hukum Acara Pidana Indonesia*. In *Hukum Acara Pidana Indonesia*.
- 3) Awad, E. M. (2003). *Electronic Commerce: From Vision to Fulfillment*. McIntire School of Commerce University of Virginia.
- 4) Baylis, J., and Smith, S. (2001). *The Globalization of World Politics: An introduction to international relations*. The Globalization of World Politics: An Introduction to International Relations.
- 5) Djumhana, M. (2012). *Hukum Perbankan di Indonesia*. Bandung: PT. Citra Aditya Bakti.
- 6) Hafidz, J. (2014). *Kajian Yuridis Dalam Antisipasi Kejahatan Cyber*. *Jurnal Pembaharuan Hukum*.
- 7) Hutauruk, D. M. (2020). *Peran Perbankan Sangat Besar dalam Menggerakkan Ekonomi Nasional*. Retrieved from Kontan.Co.Id website: <https://keuangan.kontan.co.id/news/peran-perbankan-sangat-besar-dalam-menggerakkan-ekonomi-nasional>
- 8) Lombard, D. (2005). *Nusa Jawa: Silang Budaya, Warisan Kerajaan-kerajaan Konsentris*. Penerbit PT Gramedia Pustaka Utama. Jakarta.
- 9) Mamudji, S. S. & S. (2004). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: PT Raja Grafindo.
- 10) Permata, G. (2018). *Tanggung Jawab Bank Atas Pelanggaran Kerahasiaan Data Nasabah Oleh Pegawai Bank*.

Bank Responsibility on Customer's Data Fraud in Indonesia

Universitas Islam Indonesia.

- 11) Shidarta, S. I. &. (2013). *Metode Penelitian Hukum Konstleasi dan Refleksi*. Jakarta: Yayasan Pustaka Obor Indonesia.
- 12) Sidik, S. (2013). Dampak Undang-undang Informasi dan Transaksi Elektronik (UU ITE) terhadap Perubahan Hukum dan Sosial dalam Masyarakat. *Jurnal Ilmiah WIDYA*, Volume 1 N.
- 13) Soemitro, R. H. (1982). *Metodologi Penelitian Hukum dan Jurimetri*. Jakarta: Ghalia Indonesia.
- 14) Suardi, S. (2011). No Title. Urgensi Convention on Cybercrime Tahun 2011 Dalam Rangka Pembentukan Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia, *Inspirasi*,. Retrieved from <https://www.neliti.com/publications/242789/urgensi-convention-on-cybercrime-tahun-2001-dalam-rangka-pembentukan-undang-unda#cite>
- 15) Sulisty, R. F. R. & A. (2017). Analisis Pemisahan Wewenang Pengawasan Lembaga Keuangan Perbankan antara Bank Indonesia dengan Otoritas Jasa Keuangan. *Privat Law*, Vol. V No.
- 16) Talumewo, F. J. (2013). Pertanggungjawaban Bank Terhadap Nasabah Yang Menjadi Korban Kejahatan Informasi Dan Transaksi Elektronik (ITE). *Lex Crimen*, Vol. 2.
- 17) Yun. (2021, April 7). Terbukti Kena Skimming, Nasabah Dapat Uang Ganti dari BRI. *CNBC Indonesia*. Retrieved from <https://www.cnbcindonesia.com/news/20210407145754-4-235976/terbukti-kena-skimming-nasabah-dapat-uang-ganti-dari-bri>
- 18) Zulf Diane Zaini. (2014). Pengalihan Fungsi Pengawasan Lembaga Perbankan dari Bank Indonesia ke Otoritas Jasa Keuangan. *Jurnal Pranata Hukum*, Vol. 9, No.



There is an Open Access article, distributed under the term of the Creative Commons Attribution–Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.