International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 10-06-2024, Accepted: 01-07-2024, Published: 24-07-2024
Volume 10, Issue 4, 2024, Page No. 95-98

Criminal responsibility for perpetrators of fraud cases through a counterfeit mobile banking application in Indonesia

Debby Hermelina, Septiana Prameswari
Department of Law, Universitas Wijaya Kusuma Surabaya, Indonesia

Abstract
The development of technology, the result of human culture, has not only positive but also negative impacts on humans and the environment. One of the increasing negative impacts is crime, especially in the form of fraud using technology. This crime is increasingly rampant online or through technological media because many people are looking for an easy and efficient way to fulfill their needs without having to spend a lot of time and money. In the face of the development of increasingly complex criminal acts of fraud, proof is a challenge for law enforcers when only referring to the provisions in the Criminal Code. This research uses normative research methods by examining national laws and regulations. The offense of fraud in electronic transactions is regulated in Article 28 paragraph [1] of the Second Amendment to UUITE, although not explicitly, there is an element of resulting in consumer losses in electronic transactions" which can be used as a basis for the criminal offense of fraud in electronic transactions basis for the criminal offense of fraud in electronic transactions.

Keywords: Criminal liability, fraud, fake mobile banking

Introduction

Currently, the flow of globalization is leading to an age full of digital technology. Digital technology, where advances in information and communication technology play a significant have a significant role. With the advancement of technology in modern life as well as the increasingly strong influence of globalization, the Internet has become a necessity for society, and for the community. In almost all aspects of life, internet connection has become a support for community activities, both in business and fulfillment of daily needs. In this digital era, electronic media has become one of the key infrastructures for conducting transactions in various business sectors, including key infrastructure to carry out transactions in various business sectors, including in banking services [1].

The provision of electronic transaction services (e-banking) through ATM, internet banking, and payment processing using debit and credit cards are the latest innovations in banking services. debit and credit cards are the latest innovations in financial service channels that shift the pattern of manual transactions from that shifting the pattern of manual transactions to transactions that rely on technology to support the growth of e-commerce, the importance of the development of internet payment systems is increasingly becoming a concern, shifting the method of from manual to online-based payment methods.

The rapid development of technology and globalization in Indonesia makes information technology have an important position in the progress of the country. In almost all parts of the world, people use the internet to help work become younger and faster. The development of information technology is also utilized by the banking sector to improve the quality of services from the banking sector by creating applications that can help customers make transactions more easily and practically. Applications made by banks are Internet banking application services commonly referred to as mobile banking [2].

Mobile banking is an application service issued by the banking sector to carry out various banking transactions through the features and menus contained in the application that can be downloaded and installed via the customer's smartphone. Mobile banking services can make it easier for customers to make various transactions more easily, quickly, and practically without the need to come to the nearest ATM branch to save time and money. In addition, transactions through mobile banking can be done anywhere and anytime without time limits. Several mobile banking features can be used by customers such as information services (balance, account mutations, interest rates, and location of the nearest branch/ATM), and transaction services (transfers, payments, bills, credit purchases, and various other features).

However, there are not only positive benefits that can be felt by the community through the development of information technology but also many negative impacts that the community must be aware of. Along with the development of information technology, criminals take advantage of technological developments to commit crimes commonly referred to as cybercrime. According to Andi Hamzah in his writing "Criminal Aspects in the Computer Field", cybercrime is a crime in the computer field that is committed illegally. In addition, the definition of cybercrime is also stated by Murti who argues that cybercrime is a term used to describe a crime using computer media or the internet. In general, cybercrime can be defined as crimes committed using electronic media and information [3]. Some of the crimes that have occurred in Indonesia are malware, pharming, phishing, cyberstalking, cyberbullying, DDOS (Distributed Denial of Service), financial crimes, and critical infrastructure attacks. Of the various types of crime models that occur in the cyber world, crimes that are rampant by utilizing information technology are fraud crimes committed online commonly referred to as online fraud. Online fraud is fraud committed using digital media or platforms to carry out its actions. In contrast to conventional fraud which is carried out in real life without

using the media, it can be concluded that the difference between online fraud and conventional fraud lies in the means or media used to commit fraud.

In general, the crime of fraud is regulated in the Criminal Code (KUHP) Article 378 which explains that fraud is an act that benefits oneself or others by using deception to hand over property, objects, money, and wealth to him. However, in the Criminal Code, both online fraud and conventional fraud are treated the same. However, in the Criminal Code (KUHP) the use of the fraud article becomes inappropriate when used in cases of online fraud, this is due to the restrictions on evidence regulated in the Criminal Procedure Code so a special law is needed that can regulate online fraud Criminal offenses [4].

Law No.19 of 2016 concerning the amendment of Law No.11 of 2008 concerning information and electronic transactions (ITE) can be a legal umbrella for overcoming and preventing criminal acts of fraud related to information technology. Article 1 paragraph [3] of ITE Law explains that information technology is a technique in collecting, analyzing, preparing, processing, and disseminating information. In addition, Article 1 paragraph [2] also explains that electronic transactions are legal actions carried out using computer systems, computer networks, or electronic media. So that this ITE Law can be used as a "cyber law" regulation in handling cases of criminal offenses related to technological developments.

In addition to the Criminal Code (KUHP) and the ITE Law, the criminal offense of fraud is related to consumer protection. Law No. 8 Year 1999 on Consumer Protection regulates all efforts to ensure legal certainty to protect consumers. Every consumer is entitled to have the right to feel safe in using and utilizing information technology in carrying out various kinds of activities from buying and selling, as well as making various kinds of payments. The Consumer Protection Law mentions consumer rights to comfort, security, and safety in consuming goods and services, so regarding the safety and comfort of customers in using Internet banking or mobile banking services is the responsibility of the bank to provide the best facilities for its services to customers.

Problems related to online fraud using internet banking or mobile banking occurred in West Java in 2022 on behalf of Bri Bank with the mode of sending or distributing notification links via short messages in the WhatsApp application to potential victims regarding the latest policy changes in transfer fees so that victims do not feel suspicious. After the victim agrees to the policy, the victim is taken to a site that is similar to the original mobile banking site from BRI-Mobile, and then the victim will fill in personal data information such as username and password after that the perpetrator will automatically take all of the victim's data to hack the victim's account. from the above case, it can be concluded that there is a need for legal efforts to overcome and prevent criminal acts of fraud by utilizing information technology [5].

Based on the above description, the author determines the title of this paper "Criminal Liability for Perpetrators of Fraud Through Fake Mobile Banking". The formulation of the problem that the author discusses is the fraud process through fake mobile banking.

Research Methods

The research method carried out in this legal research is to use the method of legislation approach (statute approach) and conceptual approach. Normative law research uses normative case studies in the form of legal behavior products, for example examining laws. The subject of study is law which is conceptualized as norms or rules that apply in society and become a reference for everyone's behaviour. So normative legal research focuses on the inventory of positive law, legal principles, and doctrines.

Discussion

Fraud Process through Fake Mobile Banking

Fraud can occur because the perpetrator sends a short message to potential victims to get feedback or reciprocity from potential victims. Fraud crimes do not only occur conventionally, but as technology develops fraud crimes can now also be in the form of digital fraud crimes or commonly referred to as online fraud which is now often rampant in society and is still a global problem.

Online fraud is fraud committed using electronic media to carry out its actions. Online fraud that currently often occurs in the banking sector by utilizing mobile banking application services, namely pharming crimes. Mobile banking is one form of facility provided by the banking sector to facilitate customers in conducting banking transactions anywhere and anytime without the need to come to the branch office. Various features of mobile banking services provided by the banking sector that can be utilized by customers using mobile banking are bill payment transactions, the latest information on interest rates, and foreign exchange rates, administration regarding changes to personal identification numbers (PIN), account or card addresses, except for cash withdrawals and deposits [6].

However, in reality, there are still many cases of abuse committed by cybercriminals. One type of cyberattack that can threaten the security of the banking world, especially in the use of mobile banking, is pharming crime. Pharming crime is a cybercrime that involves redirecting the victim to a malicious website without the knowledge or consent of the victim, the website created often looks like a suitable website like the original website of the bank. The goal of a pharming attack is to gain access to personal information from the victim, making it easier for the perpetrator to commit fraud and identity theft. [7]

Pharming attacks can occur by several methods such as manipulating the Domain Name System (DNS), changes to the host file on the user's device, the use of malware that changes DNS settings, or even through attacks on routers used by mobile banking users. Of the several cybercrimes that occur through mobile banking in Indonesia that are rampant, namely pharming crimes with the mode of mobile banking fraud via SMS or chat sent via WhatsApp media in the form of changes in admin transfer fees. Where the perpetrator sends a short message to potential victims in the form of a change in the admin transfer fee from the bank, then if the victim agrees to the change, the victim is asked to click on the site that has been created by the perpetrator and the site will direct the victim to the same mobile banking application as the original mobile banking from the bank, after the victim enters the username and password into the mobile banking application, all data and even cash in the victim's mobile banking will automatically be lost or drained by the perpetrator. Pharming crimes are considered

easy to carry out attacks in taking the victim's data, as for what makes pharming a dangerous crime when compared to other crimes this is because pharming only requires a little action from the user. There are several impacts of pharming crimes in the cyber world, namely:

- Mobile banking users are aware and have an understanding of the risks and precautions of pharming, while others have limited understanding and are less aware of the threat of pharming.
- They described hesitation and uncertainty in using the service, especially after learning about Pharming attacks.
- The importance of preventive measures implemented by mobile banking service providers, such as providing clear information about Pharming, strong identity verification, and effective protection of mobile banking user data.
- Pharming attacks harm the trust of mobile banking users.

Application of Responsibility for Perpetrators of Criminal Offences of Fraud through Fake Mobile Banking

Criminal responsibility can be called criminal liability in English which has 2 syllables namely criminal and liability which means obligation or responsibility. According to Simons, liability is an ability as a psychological condition that justifies the application of a punishment. Criminal responsibility has objective requirements that must be met which in the juridical sense is that the act must have been a criminal offence according to the applicable law. Cases of fraud committed online by utilizing electronic technology are significantly not regulated in the Criminal Code (KUHP) this is because the Criminal Code (KUHP) only regulates the article of fraud as a whole. Under Article 378 of the Criminal Code, which regulates actions that benefit themselves or others by deception and lies intending to hand over all goods or property belonging to someone to him, shall be punished with a maximum imprisonment of 4 (four) years. In addition to being regulated in the Criminal Code (KUHP), the crime of fraud relating to information and electronic transactions is also regulated by Law Number 11 of 2008 concerning Electronic Information and Transactions which was later amended into Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 which is then referred to as the Amendment to the ITE Law. Article 28 paragraph explains that every person who intentionally and without spreading false and misleading news that causes harm to consumers can be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp 1,000,000,000.00 (one billion rupiah) [8].

With the existence of laws and regulations governing Electronic Information Technology, it can provide benefits for consumers. So that it can minimize and protect consumer rights and provide a sense of security in using electronic media and other online media. Apart from through the law, preventive efforts can also be made to overcome and prevent crimes using electronic media, namely by providing socialization or news through the media which can be used as a means for the public to find out more about ITE law so that people are not easily cheated online. Other repressive efforts can also be made by reporting to the authorities related to criminal acts including online fraud which can then be given legal sanctions against the perpetrators of online fraud using the relevant articles to provide a deterrent effect to the perpetrators and provide a sense of justice for the community.

The use of criminal law can be used as a form of prevention and in overcoming the dangers and losses arising from cybercrime from the increasing development of information technology. Protection of the public interest in tackling online fraud is needed so that several actions can be taken to prevent online-based fraud attacks, especially in the use of mobile banking, namely:

- Not disclosing confidential data to other parties [9].
- Not recording and storing SMS banking codes or personal numbers in a place that is easily known by others.
- Checking the transaction carefully before confirming the transaction.
- Every time you make a transaction, it is better to wait for a few moments until you receive a response to the transaction.
- For each transaction, the customer will receive a notification message on the transaction in the form of SMS or email and check carefully the contents of the notification if there is a suspicious transaction immediately contact the bank [10].
- If you feel that your PIN has been compromised, please change it immediately.
- If the GSM SIM Card is lost or stolen or has been transferred to another party, immediately notify the nearest bank branch office or contact the bank's call center.
- Always be careful with applications on the internet that are spam or malware that may steal personal data.
- Do not conduct Internet transactions in public places.
- Do not forget to log out after completing the transaction.

Fraud, as contained in the article above, is still conventional in nature, meaning that fraud generally occurs in real life and covers a variety of situations [11]. However, the use of this article becomes inappropriate when applied to cases of fraud in electronic transactions in cyberspace. This is due to the restrictions on evidence set out in the Criminal Procedure Code (hereinafter referred to as KUHAP) as well as the complex jurisdictional issues that arise in the handling of cybercrime cases.

Conclusion

Based on the discussion above, it can be concluded that online fraud is fraud committed by utilizing information technology as a means. Legal regulation of online fraud in the form of pharming needs to require special laws that regulate and can be applied so that victims can obtain fair legal protection and feel safe in using mobile banking. In addition, it can also provide a deterrent effect to the perpetrators of fraud so that there will be no more victims of misused technological developments.

Reference

1. Aditama R. Penegakan hukum cyber crime terhadap tindak pidana pencurian uang nasabah dengan cara pembajakan akun internet banking lewat media sosial. Wajah Hukum, 2021, 118-125.
2. Delvyan NP, Robekha J. Analisa yuridis dalam kasus kejahatan siber terhadap internet banking di indonesia. Jurnal Pendidikan, 2023.

3. Hondro ER. (n.d.). pengaruh penggunaan mobile banking terhadap minat nasabahdalam bertransaksi menggunakan technology acceptancemodel.
4. Ibrahim MY, Putri H. Perlindungan Hukum Terhadap Korban Penipuan Online Shop Melalui Jaringan internet. Jurnal Imiah fenomena, 2016.
5. Kesuma IG, Widiati IA, Sugiartha IN. Penegakan Hukum Terhadap Penipuan Melalui Media Elektronik. Jurnal Preferensi Hukum, 2020.
6. Ketaren E. Cybercrime, Cyber Space, Dan Cyber Law. Jurnal Times, 2016, 35-42.
7. Marita LS. (n.d.). Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia.
8. Muhammad FE, Beniharmoni H. Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web. Usm law review, 2023
9. Pinto MY. (n.d.). Penegakan Hukum Terhadap Tindak Pidana Penipuan Dengan Modus Electronic Cash Di Kepolisian Resor Kota Pekanbaru.
10. Rahmad N. Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online. Jurnal Hukum Ekonomi Syariah, 2019.
11. Utin IP. Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police di Indonesia. Mimbar Jurnal Hukum, 2021.