E-ISSN: 2962-2816 | P-ISSN: 2747-1985
JOURNAL OF LAW, POLITIC AND HUMANITIES (JLPH)
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v4i3
Received: 21 March 2024, **Revised:** 30 March 2024, **Publish:** 19 April 2024

Law Enforcement for Fraud Offenders on behalf of Banks Through Online According to Islamic Criminal Law

Rabullah Putra[1], Syaddan Dintara Lubis[2]
[1]Hukum Pidana Islam, Universitas Islam Negeri Sumatera Utara, Indonesia
Email: rabullah0205193136@uinsu.ac.id
[2]Hukum Pidana Islam, Universitas Islam Negeri Sumatera Utara, Indonesia
Email: Syaddandintaralbs@uinsu.ac.id

Corresponding Author: rabullah0205193136@uinsu.ac.id

Abstract: This research aims to find out the modus operandi of criminal fraud on behalf of banks through online, to find out law enforcement for fraud perpetrators on behalf of banks through online at the North Sumatra Regional Police, and to find out the review of Islamic criminal law in fraud cases on behalf of banks through online. This research uses a qualitative empirical research strategy in the field of law. Interviews with members of the North Sumatra Regional Police became the main data source, while literature surveys of online journals, papers, and articles related to fraud legislation became secondary data. Data reduction, data presentation, and conclusion drawing are the three stages of qualitative data preparation. Article 378 of the Criminal Code can be used to regulate the crime of online fraud, according to the above study. To strengthen the legal basis, Article 28 paragraph (1) of the ITE Law can be followed. Islamic criminal law, which is based on hadith and the Quran, does not provide clear guidelines on how to deal with internet fraud involving banks. Islamic law includes general principles that should be followed, and their application depends on the interpretation of local scholars or religious authorities. In the case of online fraud on behalf of a bank, which is included in the crime of fraud, it can be subject to ta'zir punishment such as a stern warning, a material fine whose amount is adjusted to the victim's loss, imprisonment, flogging, or also exile from society for a while.

Keyword: Law Enforcement: Online Fraud: Banks: Islamic Criminal Law

INTRODUCTION

Various areas of human life, including education, economics and politics, are greatly affected by the rapid advancement of technology today. Information and communication technology is one type of technology that we use in our daily lives. In particular, the way people interact and share information is changed by this type of mobile phone and its various advanced features. Short message service (SMS) capability is one of the options available to us. Normally, this function is used to facilitate the transmission of short messages; however,

over time, criminals have taken advantage of this service feature. This is known as cybercrime.

Financial institutions, such as banks, play an important role in the economy of many countries, including Indonesia. As stated in Chapter 1 Article 1 and paragraph (2) of Law No. 10 of 1998 concerning the amendment of Law No. 7 of 1992 concerning Banking, a Bank is defined as a business entity that collects public deposits and then lends or otherwise provides these funds to the public with the aim of improving living standards. Good deal.

In the ever-growing digital era, online banking services have become a key tool for people to manage their finances. The use of online banking services has become integral to everyday life, making financial access and transactions easier However, increasing concerns regarding online scams masquerading as banks marks a trend that needs to be watched closely. Fraudsters are cleverly utilizing technology to deceive and harm the use of banking services.

There are many modes of online fraud that often occur. Examples include ATM skimming, where illegal devices are installed to steal credit/debit card information. Then, smishing or fraud through electronic messages in the form of SMS that often occurs lately. The perpetrators send a message with a link to direct the victim to false information, where the perpetrator also provides a fake cell phone number. Usually this case is masked by providing false information such as the victim being selected as a winner in a lucky draw, so the perpetrator will ask for confirmation to send funds as a form of aid disbursement, such as customer information. Then, the perpetrators will try to access the victim's personal information to be robbed.

Based on the results of OCBC NISP research, there are several types of fraud that are often carried out by fraudsters, namely phishing or types of fraud through online or electronic, in the form of messages via email, social media, or SMS. Then there is vishing (voice phishing), which is a type of fraud via voice technology (telephone). The third is impersonation, which is a type of fraud with the mode of offering something to get personal information so that the perpetrator accesses the number to the victim's personal information and account number and then the perpetrator drains money from the victim's account.

Laws are needed to combat the many cases of fraud. The law of a society is a set of rules and regulations, including commands and prohibitions. Law enforcement against perpetrators of online fraud on behalf of banks is a serious challenge that requires a quick and efficient response.

It is important to realize that online fraud not only results in financial loss but also undermines public trust in digital banking services. The government has regulated the provisions in Law No. 11 of 2008 on ITE which is expected to make the use of technology more manageable and can be used by the public in moderation. Although the ITE Law does not specifically regulate the crime of fraud, with regard to the losses incurred in online transactions can be seen in Article 28 paragraph (1), that "every person intentionally, and without the right to spread false and misleading news that results in consumer losses in electronic transactions."

According to Kaspersky data, 1.6 million phishing attempts occurred in Southeast Asia in January-June 2020. Of this total, 749.9 thousand cases occurred in Indonesia. These criminals will send links that lead us to download dangerous programs, on the other hand, people's digital literacy is still low, and of course it is a public concern to educate the public.

In 2021, there was a significant increase in online fraud cases on behalf of banks compared to 2020, up to 78%. Throughout 2022, the mode of fraud by utilizing the name of the bank is also still rampant in Indonesia. Semuel Abrijani Pangerapan, Director General of Informatics Applications at the Ministry of Communication and Information, said that the number of victims in 2022 of fraud on behalf of banks reached 130 thousand people. Based

on data from the Financial Services Authority in November 2022, at least 6,756 reports were received from the banking sector.

It is estimated that the trend of increasing cases like this will continue until 2023 considering that more and more people are using digital banking services. Some sources estimate that online fraud cases related to financial technology, including on behalf of banks, could reach 60-70% of the total cybercrime in Indonesia by 2023. From Kemkominfo's information, there were 1,730 online fraud contents from August 2018 to February 16, 2023, from this case there were recorded losses of up to Rp 18 trillion rupiah experienced by victims. In 2023, the Financial Services Authority has completed at least 17 investigation case files on financial crime cases originating from the banking sector, with 4 Non-Bank Financial Industry cases and 13 more banking cases. Whereas in October, investigators from the Financial Services Authority were handling 26 cases that were still in the investigation stage, with details of 14 cases originating from banking, 4 cases from the capital market, and 8 cases from the Non-Bank Industry.

In North Sumatra alone in 2023 there were at least 121 cases of online fraud on behalf of banks. North Sumatra Police in handling online fraud cases on behalf of banks, conduct account profiling. Account profiling of accounts suspected of being perpetrators of fraud. Then the investigator will profile the suspected account, by looking for the perpetrator's personal information. The next step is to verify whether the account is actually officially registered on behalf of the bank or not.

In this case, a case of online fraud on behalf of a bank was experienced by a 67-year-old man, Irwan Gema from Malang City, who lost Rp 549 million after he clicked on a PDF application link sent via Whatsapp message. This case has been reported to the bank, but in this case the bank did not provide a solution, instead blaming Irwan by considering this carelessness of the customer.

Cases that often occur in Medan, where fraud starts with a message via WhatsApp or SMS by sending a text message in the form of a link. The fraudster with the link can hack and know the target's cellphone number and password by convincing the target with the seduction of his words that the target is interacting with the bank.

In this context, law enforcement plays a key role in protecting the public and maintaining the integrity of the banking sector. Nonetheless, challenges continue to evolve along with technological advancements. Therefore, an in-depth analysis of law enforcement strategies, consumer protection, and prevention efforts is crucial in addressing the threat of online fraud.

The rise of fraud cases on behalf of banks through online needs to be prevented and dealt with firmly according to HPI online fraud includes jarimah ta'zir because it harms victims and disturbs the community. Preventive efforts that can be implemented include socializing the dangers of online fraud, increasing the ability of the people to detect fraud, and regulations that prohibit fraudulent practices under the guise of banks. Perpetrators of online fraud are subject to ta'zir punishment in the form of corporal punishment and fines. Corporal punishment can be flogging or imprisonment, with fines as material compensation for victims. Plus additional penalties such as announcing the identity of the perpetrator. With the above case, this is the motivation for the author to carry out further research on "Law Enforcement for Fraud Offenders on behalf of Banks Through Online According to Islamic Criminal Law".

METHOD

Empirical legal research included in this study is legal research that relies on data collected directly from the public, such as through interviews or observations of their actions in the real world. Researchers use field research, namely physically visiting the location of the object of research to collect direct information on the application of the Criminal Code

Article 378. This research falls into the category of qualitative research which is defined as an approach to data collection that does not rely on numerical or symbolic representations. The descriptive nature of this research means that the findings will be explained based on the researcher's own analysis and observations.

Primary and secondary data sources were used to collect information for this study. Data collected through in-depth interviews with knowledgeable individuals or data collected directly from the field are examples of primary sources. Polda Sumut provided most of the data used in this research. The next step was to supplement the primary data with secondary materials collected from books. Desk research, including reading books, journals, or materials related to criminal fraud laws and regulations found online, constitutes secondary data in this research.

The term "data collection" refers to the process of gathering information in a structured and methodical manner. There is always a relationship between research topics and data collection techniques. The issue dictates the action and impacts the data collection technique. Interviews and question and answer sessions with members of the North Sumatra Regional Police were the means by which the author gathered information for this research. As part of its preparation, this research used a qualitative analysis approach, which is a way of processing the data obtained by studying it based on field conditions. After data collection, the data reduction method was used. This involves selecting and concentrating on simplifying the raw data derived from field notes, and finally, the data is presented in a structured way that allows conclusions to be drawn. Finally, the research will culminate in the development of conclusions, which involves using the facts gathered to create a framework or conclusion.

RESULTS AND DISCUSSION

Modus Operandi of Fraud on behalf of the Bank through Online

Illegal conduct is conduct that is prohibited by law and carries the possibility of repercussions, in the form of certain penalties, for those who disobey the prohibition. The root word for deceptive or dishonest behavior or speech is deceit, which is also the root word for fraud. Because it causes harm to another individual, fraud is considered a criminal offense. Whether a case involves civil or criminal fraud is often stated in the law; the main difference between the two is the greater standard of proof required in criminal proceedings.

Article 378 of the Criminal Code deals with the crime of fraud in its fullest form, which is recognized and termed bedrog. Objective and subjective factors both play a role in this crime of fraud. The objective component means the use of instruments of persuasion or mobilization to influence or affect other individuals, such as deception, false identity, fabricated circumstances, and a series of misleading statements. Meanwhile, the subjective component is breaking the law for the benefit of oneself or others. The perpetrator does not need to have malicious intent for the law to be violated. It can be concluded that the crime of fraud in its principal form regulated in Article 378 of the Criminal Code is a criminal offense, but this conclusion is based on the criterion that the perpetrator must have a legal intention to benefit himself or others.

The following is developed by R. Soesilo related to the offense of fraud as outlined in Article 378 of the Criminal Code;

1 Fraud is the name given to this type of crime, and the roles played by the perpetrators are:
   a. Encouraging another person to share his money, take out a loan, or write off his debt
   b. By using persuasion, one can obtain benefits for themselves or others at the expense of their rights
   c. The persuasion is by using:
      1) A false name or false circumstances
      2) Deceit
      3) A series of false words

2 Persuasion is the art of subtly influencing others to act in a way that they would regret if they knew the truth.
3 Assuming all other conditions are met, convincing someone to hand over their property can also be considered fraud as there is no requirement that the property belongs to someone else.
4 As with theft, the rules outlined in paragraph 367 also apply to fraud even if it occurs within the family. Article 394 of the Criminal Code.

Chapter XXV of Book II of the Penal Code regulates the first criminal offense of fraud, which is the unlawful giving of advantage to oneself or another person through the use of a false name or dignity, deception, or a series of false words to induce another person to commit a wrongful act of giving something to oneself. The Criminal Code, namely articles 378-395 of book II chapter XXV, regulates fraud.

The crime of fraud in general is in the form of fraud in the main form (standard form) contained in article 378, the formulation of which is, "whoever, with the intention of benefiting himself or another person against the right, either by using a false name or a false situation, either by means of tricks and deceit, or by false words, persuades someone to give something, make a debt or write off a debt, shall be punished by fraud, with imprisonment for a maximum of four years".

Cybercrime is regulated by Law No. 11/2008 on Electronic Information and Transactions (UU ITE). This law complements the Criminal Code which contains provisions on fraud. Everything from information and electronic transactions to criminal threats and prohibited topics in "cyberspace" are included in this regulation.

As part of the study of computer-related fraud, the category of unlawful content crimes includes the crime of utilizing the internet to commit fraud. In contrast to computer-related fraud, which is defined as fraud or deception committed for the purpose of obtaining personal gain or inflicting harm, unlawful content is the practice of posting inaccurate, unethical, or misleading information online in order to commit a crime or disrupt public order apart from that.

In theory, online fraud is no different from traditional forms of fraud. The utilization of electronic systems (computers, internet, telecommunication equipment) is the only differentiator between the two methods. The Criminal Code, which is based on the Electronic Transaction Law, is still the only source of law that deals with this kind of fraud, which is complicated in committing the crime or often referred to as modus operandi. Modus operandi comes from Latin, which means to do something. Various modes of online fraud often appear and the perpetrators are increasingly neat in carrying out their actions. The same thing is certainly done by online fraudsters on behalf of banks. Some modus operandi that often occurs among the public related to criminal acts of fraud on behalf of banks through online, such as:

1 Phishing

In which, the perpetrator will send an email or message pretending to come from the bank. The email may contain a link or attachment that, if the victim opens or downloads the attachment, will steal the victim's personal data and internet banking login information.

2 Account break-in

The perpetrator breaks into the victim's account by exploiting internet banking security loopholes or stealing the victim's login data. After that, the perpetrator transfers money from the victim's account to the perpetrator's account.

3 Creation of fake websites

The perpetrator creates a site that is similar to the original internet banking site, then the perpetrator lures the victim to log in on the fake site so that the victim's login data can be stolen.

4 Computer hacking/Sniffing

The perpetrator hacks into the victim's computer to steal personal and financial information including internet banking login data, then misuses the data to transfer the victim's money.

5 Fake phone calls

The perpetrator contacts the victim and pretends to be from the bank. The perpetrator asks the victim to perform activities such as login, re-activation, or card replacement under the pretext of security. The goal is to steal the victim's personal data.

Law Enforcement for Online Fraud Perpetrators at the North Sumatra Regional Police

In trying to find the parties responsible for fraudulent acts, law enforcement officers often face several challenges and obstacles. The fraudulent behavior is charged with violating Article 378 of the Criminal Code which regulates fraud, or Article 28 of the ITE Law paragraph (1) which regulates the dissemination of misleading and untrue news that is detrimental to customers.

A country's ability to successfully enforce relevant laws is a hallmark of the realization of the rule of law. The honesty of rule makers, rule breakers, and the regulated society as a whole are vulnerable to the maximum consequences of law enforcement actions or inaction. So, it can be said that the way law enforcement handles all legal relationships is not ideal.

Soerjono Soekanto said there are five factors that have an impact on existing law enforcement, namely:

1. Legal factors, Legal considerations, factors that come from the law or the law in question. This includes situations when there are no implementing regulations that can be applied, or when the language of the regulation is unclear, thus causing different interpretations of what is written in the regulation.
2. Law enforcement factors, Elements relating to law enforcement, or aspects stemming from law formulators and enforcers. In this case, each branch of law enforcement has its own skills and expertise. Therefore, the authority given by the state to law enforcement is diverse and different. Yet many police officers face considerable political interference as they carry out their duties. As a result, the law favors one party over another.
3. Facilities that accommodate law enforcement. The place where law enforcers can carry out their duties. In order to carry out their duties effectively, law enforcement agencies must have adequate facilities and resources, such as qualified personnel, trustworthy organizations, and your equipment.
4. Community factors, Considerations relating to society, including the environment in which the law is implemented.
5. Cultural factors, The contribution of human endeavor, imagination, and emotion in social life; these are cultural aspects.

There is a strong interdependence between the five criteria listed above. A decline in performance due to one component will almost certainly impact the others.

Although the National Police has made some efforts to crack down on internet fraud, it is clear that there are still many circumstances that make this crime difficult to prosecute. The author outlines five variables that hinder the progress of this research, namely:

a. Proving the crime of online fraud

Due to the lack of proper evidence outlined in Article 184 of the Criminal Procedure Code, it is challenging to apply the criminal evidence scheme against online fraud perpetrators when relying on the provisions of the Criminal Procedure Code to prove non-conventional fraud. The ITE Law is more suitable for proving the guilt of online fraud perpetrators as it has certain limitations that address offenses involving electronic transactions.

b. Infrastructure in support of the evidentiary process

Poor infrastructure is also a potential obstacle to effective law enforcement. As the techniques used by cybercriminals to commit online fraud continue to evolve, law enforcement agencies must have the resources they need to deal with this kind of crime. In addition, criminals register fake or real phone numbers that belong to other people, as well as account numbers that may be used by other people.

c. Limited human resources in the law enforcement process

There is an urgent need to update law enforcement training to keep pace with the increasing complexity of cases using digital media. Simply put, it is reasonable to assume that the talents of modern police investigators are not comparable to those of their predecessors. To reduce the occurrence of new crimes, law enforcement officers must adjust to the ever-changing landscape of society and technology. In addition, law enforcement officers should put more effort into understanding the articles in the current positive legislation to avoid different interpretations when it comes time to use these articles against online fraud perpetrators.

To protect the general public, regulations governing internet fraud are urgently needed. Among the many prohibited acts involving the exploitation of information technology is internet fraud committed on behalf of banks. The amendment to Law 11 of 2008 on ITE (Law No. 19 of 2016) does not explicitly mention internet fraud as a crime. There is no suggestion of fraud in these writings. It is explained that the basis for online fraud is contained in Article 28 paragraph 1 of the ITE Law "Every person who intentionally and without right spreads false and misleading news that results in consumer losses can be punished with 6 years imprisonment or a fine of 1 billion rupiah". Article 28 paragraph (1) refers to Article 378 of the Criminal Code which only focuses on fraud.

The elements contained in Article 28 paragraph (1) of the ITE Law have certain similarities with the traditional criminal offense of fraud outlined in Article 378 of the Criminal Code. However, the ITE Law also has its own uniqueness, such as the ability to recognize evidence, the use of electronic media, and the expansion of jurisdiction. Law No. 8 Year 1999 which regulates consumer protection is a complement to the requirements of Article 28 paragraph (1) of the ITE Law. A consumer protection system that offers legal certainty and transparency in accessing information is the goal of both initiatives, while increasing consumer awareness and empowering consumers to take action independently are the objectives of both initiatives.

One example of a case that often occurs related to fraud on behalf of banks online is that the fraudster sends a message via WhatsApp or SMS by sending a message in the form of a link. Then the target opens the message and clicks on the link sent by the fraudster, from here the fraudster will interact with the target by trying to convince the target that the one who sent the message is the bank. After that, the target is directed to the link sent, asked to provide a cellphone number and password, which can then be accessed by the fraudster. The result is a fraudulent withdrawal of funds or theft from the target's bank account.

lptu Benny Saragih as an Assistant Investigator at the North Sumatra Police explained that the mode used by online fraudsters can be in the form of offering goods (for sale), this form of fraud usually sends goods but is different from the goods previously offered, or it can be by selling words, meaning that the fraudster will seduce the victim with words to realize the wishes of the fraudster. Scammers often use modus operandi involving phishing techniques, where they create fake websites that mimic the official look of the bank. They may also use fake emails or text messages to request personal information or bank account logins.

Then how to overcome online fraud cases on behalf of banks that are rampant in the community? The North Sumatra Police explained that there are two ways to deal with these cases, namely:

a. By conducting an investigation, namely an investigation by looking for an irregularity whether it is a criminal offense or not.
b. By conducting an investigation, namely whether it is true that someone has committed a crime or not.

In the process of investigation and investigation, the police will examine witnesses and related institutions. It is explained that the police are not obliged to cooperate with a financial institution or bank in detecting and overcoming online fraud on behalf of the bank, but the police can cooperate if there is something that makes it possible to conduct investigations and investigations in order to collect evidence.

It is not uncommon for obstacles and barriers to be encountered by the police when conducting investigations or investigations. This is because in this process it takes a long time to process witnesses, perpetrators, and also victims who have become targets of online fraud on behalf of banks. Nevertheless, the efforts made by the police have paid off by being able to arrest the perpetrators of fraud.

As a result of violating Article 28 paragraph (1) of the ITE Law as stated in Article 45 A paragraph (1) of the same Law, imprisonment for a maximum of six years and/or a fine of Rp1,000,000,000.00 (one billion rupiah). . Article 28 paragraph (1) of the ITE Law does not mandate the element of benefiting oneself or others as required in Article 378 of the Criminal Code, and this is one of two paragraphs that distinguish the ITE Law from the Criminal Code.

Review of Islamic Criminal Law Against Fraud Cases on behalf of Banks Through Online

In Islamic criminal law, the crime of fraud is considered a serious offense. Although Islamic criminal law is based on shari'ah law and can vary between different countries or schools of thought. The act of fraud can involve various forms including fraud in trade, finance, or public affairs. Islamic criminal law defines punishment as retribution that aims to safeguard the interests of society in response to violations of sharia regulations.

Islamic law has principles that include business ethics and prohibitions against fraudulent acts. In the context of online fraud on behalf of banks, there are several principles under Islamic law that are most relevant, namely:

1. Haram (prohibited): Fraudulent acts are considered haram in Islam. Lying, manipulation, and the use of dishonest means in business and transactions are forbidden.
2. Amanah (trust): Islam encourages trust in every transaction. Falsely representing the bank may be considered a breach of trust.
3. Usury (interest): Fraudulent practices involving usury (interest) are also considered a violation of Islamic law. Online transactions that involve elements of usury or unauthorized profits can be considered as actions that are against the principles of sharia.
4. Transparency and fairness: Islam encourages transparency and fairness in business and transactions. Using dishonest means on behalf of the bank may be considered a violation of these values.
5. Ghibah (backbiting): Accusing or saying something untrue about another party, such as on behalf of the bank, can be considered as an act of ghibah or defamation, which is also avoided in Islam.

In the context of online fraud on behalf of banks, it is recommended that Muslims adhere to the principles of Islamic business ethics and avoid all forms of fraud. However, the legal approach to the crime of online fraud in the name of a bank may vary and be implemented in a particular country or jurisdiction.

Islamic criminal law, which is derived from the Qur'an and hadith, does not specifically regulate online fraud on behalf of banks. Islamic law includes general principles that must be followed, and their application depends on the interpretation of local religious scholars or authorities. However, there are principles in the Quran and hadith that are relevant

to business ethics, honesty, and the prohibition against fraud.

In the hadith of the Prophet, which means: "There are 73 doors to usury, the least of which is like one who commits adultery with his mother. And the most usury is the honor of a Muslim." (H.R. Hakim 2259 and authenticated by Adz-Dzahabi). This hadith explains how serious the prohibition of usury is in Islam. As well as giving a warning about the moral consequences and honor of a Muslim who is involved in usury practices. Therefore, as a Muslim it is important to stay away from all forms of usury to maintain honor and integrity as a Muslim.

When viewed in terms of sharia, fraud is the same as lying where this is included in the group of hypocrites. Because in lying to someone there is certainly an element of hypocrisy, which in the context of online fraud on behalf of the bank, the perpetrator will trick the victim with his trickery. In the Qur'an Surah An-Nisa verse 145 which means "Verily the hypocrites (are placed) at the lowest level of hell. And you will never find a helper for them". If the punishment for stealing other people's property is death, as is the case for unbelievers, then the punishment for hypocrites is at least death, as explained in this verse, which equates hypocrites with unbelievers.

The term "jarimah" can mean any number of things that are forbidden. In Islamic law, an act is considered a jarimah if it causes harm to another person or society, whether the harm is physical, financial, social, reputational, or related to the rules. In the context of online fraud on behalf of banks that do not yet have a definite punishment or have not been determined by shara' legal provisions, this phenomenon is included in jarimah ta'zir. Jarimah ta'zir is a jarimah that is not mentioned more concretely in the form of actions and punishments in the Qur'an and also in the Sunnah. Jarimah ta'zir is a term in Islamic criminal law that refers to jarimah (criminal offense) whose punishment is left entirely to the discretion of the ruler (ulil amri). Ta'zir is different from the hadd and qisas punishments that have been determined by sharia. Ta'zir punishment is flexible and aims to provide a deterrent effect and maintain the public interest.

In Al-Quran Surah An-Nisa verse 29 mentioned:

مِنْكُمْ ۚ وَلَا تَقْتُلُوا أَنْفُسَكُمْ ۚ إِنَّ اللَّهَ يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ تِجَارَةً عَنْ تَرَاضٍ كَانَ بِكُمْ رَحِيمًا

Meaning: "O you who believe! Do not eat each other's wealth by false means, except in a trade that is consensual between you..." (QS. An-Nisa: 29)This verse prohibits all forms of false transactions, including fraud in business dealings.

In the hadith, the Prophet (peace and blessings of Allah be upon him) said:

الْمُسْلِمِ لَا يَظْلِمُهُ وَلَا يُسْلِمُهُ، عَنْ أَبِي هُرَيْرَةَ رَضِيَ اللَّهُ عَنْهُ قَالَ: قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ: الْمُسْلِمُ أَخُو عَنْ مُسْلِمٍ كُرْبَةً فَرَّجَ اللَّهُ عَنْهُ كُرْبَةً مِنْ كُرَبِ يَوْمِ الْقِيَامَةِ، وَمَنْ سَتَرَ مَنْ كَانَ فِي حَاجَةِ أَخِيهِ كَانَ اللَّهُ فِي حَاجَتِهِ، وَمَنْ فَرَّجَ مُسْلِمًا سَتَرَهُ اللَّهُ يَوْمَ الْقِيَامَةِ.

Meaning: "A Muslim is a brother to another Muslim. He should not oppress him and should not hand him over (to the enemy). Whoever fulfills the needs of his brother, Allah will fulfill his needs. Whoever removes a Muslim's hardship, Allah will remove his hardship on the Day of Resurrection. Whoever covers the shame of a Muslim, Allah will cover his shame on the Day of Resurrection." (HR. Bukhari)This Hadith emphasizes the prohibition of oppressing and cheating fellow believers.

So it can be concluded that online fraud is a wrongful act that is prohibited in Islam. The perpetrator may be subject to ta'zir punishment according to the decision of the ulil amri. The goal is to deter him and not repeat his actions. In the case of online fraud on behalf of a bank, which is included in the crime of fraud, it can be subject to ta'zir punishment such as a

stern warning, a material fine whose amount is adjusted to the victim's loss, imprisonment, flogging, or also exile from society for a while. In administering the ta'zir punishment, the ruler can determine the ta'zir punishment individually or a combination of several punishments in accordance with considerations of deterrent effect and justice. The more detrimental the victim, the more severe the punishment.

CONCLUSION

Based on previous studies, it is found that Article 378 of the Criminal Code can be used to regulate online fraud, and Article 28 paragraph (1) of the ITE Law can be used to strengthen the legal basis. In Islamic criminal law, which comes from the Quran and hadith, there is no specific explanation that regulates online fraud on behalf of banks. Islamic law includes general principles that must be followed, and their application depends on the interpretation of local scholars or religious authorities. In the context of online fraud on behalf of banks, there are several principles according to Islamic law that are most relevant, namely haram, ribawi, and transparency and justice, as well as ghibah.Online fraud is an unlawful act prohibited in Islam. The perpetrator may be subject to ta'zir punishment according to the decision of the ulil amri. The goal is to deter him and not repeat his actions. In the case of online fraud on behalf of banks, which is included in the crime of fraud, it can be subject to ta'zir punishment such as a stern warning, a material fine whose amount is adjusted to the victim's loss, imprisonment, flogging, or also exile from society for a while.

REFERENSI

Aswan, *Tindak Pidana Penipuan Berbasis Transaksi Elektronik* (Guepedia, 2019)

Febriana, Annisa, 'Efektivitas Hukum Alat Bukti Elektronik Dalam Pemeriksaan Bukti Di Pengadilan Tata Usaha Negara', *Jurnal USM Law*, 6.1 (2023)

Finaka, Andrean W., 'Maraknya Penipuan Di Era Digital', *Indonesiabaik.Id*, 2023 <https://indonesiabaik.id/infografis/maraknya-penipuan-di-era-digital> [accessed 29 February 2024]

Gulo, Ardi Saputra, 'Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik', *Junal PAMPAS*, 1.2 (2020)

Gunadi, Ismu, and Jonaedi Efendi, *Hukum Pidana* (Jakarta: Kencana, 2014)

Gunawan, Hendra, 'Tindak Pidana Penipuan Dalam Perspektif Fikih Jinayah', *", Jurnal El-Qanuny*, 4.2 (2018)

Harefa, Safaruddin, 'Penegakan Hukum Terhadap Tindak Pidana Di Indonesia Melalui Hukum Pidana Positif Dan Hukum Pidana Islam', *Jurnal UBELAJ*, 4.1 (2019)

Herman, *Pengantar Hukum Indonesia* (Makasar: Badan Penerbit UNM, 2012)

Indonesia, 'Banyak Kasus Perbankan, Bank Mega Syaiah Peringatkan Hal Ini', *CNBC Indonesia*, 2023 <https://www.cnbcindonesia.com/market/20231012063822-17-479868/banyak-kasus-perbankan-bank-mega-syariah-peringatkan-hal-ini>

Indonesia, Republik, *Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Pasal 28 Ayat (1) Bab VII*, 2008

Karim, Endang Tri Pratiwi dan LM, 'Penerapan Pasal 28 Ayat (1) Undang-Undang Informasi Dan Transaksi Elektronik Dalam Tindak Pidana Penipuan Bisnis Online', *Jurnal Multidisipliner Bharasumba*, 2.3 (2023)

Maulidya, Gita Putri, and Nur Afifah, 'Perbankan Dalam Era Baru Digital: Menuju Bank 4.0', *Proceeding Seminar Bisnis*, V (2021)

Muhammad, Abdul Kadir, *Hukum Pidana* (Bandung: PT. Citra Aditya Bakti, 2004)

Muslich, Ahmad Wardi, *Pengantar Dan Asas Hukum Pidana Islam* (Jakarta: Sinar Grafika, 2004)

Nazir, Mohammad, *Metode Penelitian*, 3rd edn (Jakarta: Ghalia Indonesia, 1988)

Nurhayati, Yati, 'Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum', *Jurnal*

Penegakan Hukum Indonesia, 2.1 (2021)
Rahmad, Noor, 'Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online', *Jurnal Hukum Ekonomi Syariah*, 3.2 (2019)
Rahmanto, Tony Yuri, 'Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik', *Jurnal Penelitian Hukum De Jure*, 19.1 (2019)
Samudra, Anton Hendrik, 'Modus Operandi Dan Problematika Penanggulangan Tindak Pidana Penipuan Daring', *Mimbar Hukum: Jurnal Berkala Fakultas Hukum Universitas Gadjah Mada*, 31.1 (2019)
Sindo, 'Waspada Penipuan Perbankan, Jaga DataPribadi', *KoranSindo*, 2022 <https://nasional-sindonews.com/read/967669/16/waspada-penipuan-perbankan-jaga-data-pribadi-1670897557> [accessed 29 February 2024]
Sitompul, Josua, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana* (Jakarta: Tatanusa, 2012)
Soesilo, R., *Kitab Undang-Undang Hukum Pidana* (Bogor: Politeia, 1991)
Sudoyo, Wahyu, 'Catatan Kominfo, Korban Penipuan Online Capai 130 Riu Pada 2022', *InfoPublik*, 2023 <https://infopublik.id/kategori/nasional-sosial-budaya/715547/catatan-kominfo-korban-penipuan-online-capai-130-ribu-pada-2022> [accessed 29 February 2024]
Sugiyono, *Metode Penelitian Kuantitatif Kualitatif Dan R&D* (Bandung: Alfabeta, 2014)
Sumawarni, Sri, 'Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif', *Jurnal Pembaharuan Hukum*, 1.3 (2014)
Takanjanji, Jefri, 'Merefleksi Penegakan Hukum Tindak Pidana Penipuan Online', *Jurnal Kajian Dan Penelitian Hukum*, 2.2 (2020)
Tim Penyusun, '5 Modus Penipuan Online Dan Cara Melaporkannya Ke Polisi', *Hukum Online* <https://www.hukumonline.com/berita/a/modus-penipuan-online-lt6172286b2cb57> [accessed 29 February 2024]
Uswah, 'Banyak Penipuan Mengatasnamakan Bank', *Um-Surabaya*, 2022
Wibowo, Danang Ari, 'Penegakan Hukum Bagi Pelaku Kejahatan Terhadap Benda Cagar Budaya Di Kota Surakarta', *Jurnal Wacana Hukum*, 23.1 (2017)
Zabindin, 'Analisis Penegakan Hukum Tindak Pidana Penipuan Online Di Indonesia', *Jurnal Spektrum Hukum*, 18.2 (2021)