Legal Compliance for Consumers in Dealing with Cases of Account Tampering in Digital Banking Services

Istna Kamelina Fitrotinisak, Rahayu Mardikaningsih, Elly Christanty Gautama, Sulani, Yeni Vitrianingsih

Sunan Giri University of Surabaya, Indonesia

R E S E A R C H I N F O

Research history:
Received 6 October 2022
Revised 23 November 2022
Accepted 11 December 2022

Key words:
Cybercrime,
Account tampering,
Digital banking,
Legal compliance,
Supervision,
Financial services authority,
Consumer protection.

A B S T R A C T

Account tampering through digital banking services has become a significant problem in Indonesia. Although regulations such as the ITE Law and policies from the Financial Services Authority (OJK) have been implemented, the implementation of supervision and enforcement of these cases is still limited. This research examines how legal certainty and supervision mechanisms in the digital banking sector can provide maximum protection for customers. The research found that stronger coordination between supervision agencies and the implementation of more advanced security technologies in digital transaction systems are needed to reduce the loopholes exploited by criminals. Clear enforcement of sanctions and recovery of losses for customers are also very important to build public trust in the digital banking system. With the strengthening of the legal system, stricter supervision, and education of the public, it is hoped that digital banking will be safer and protect consumer rights more effectively.

INTRODUCTION

The rapid development of digital technology in recent decades has brought about significant changes in people's lives, including in the banking sector. This digitalization makes it easier for people to make transactions anytime and anywhere, without the need to come to the bank office. Services such as internet banking and mobile banking are innovations that increase efficiency, convenience, and accessibility for consumers. Digital banking services are now a practical and efficient solution for financial transactions, making it easier for consumers to carry out various activities such as transfers, bill payments, and balance checks without having to visit a physical bank.

Before the era of digitalization, banking transactions generally had to be done at a bank office or Automatic Teller Machine (ATM). Today the entire process can be completed in seconds through digital devices, such as mobile phones or computers. This provides significant convenience for consumers, where they are no longer limited by time and location. This shift allows people to more easily fulfill their financial needs, which in turn expands access to banking services for various groups (Dandash et al., 2007). Along with this convenience comes various security risks, one of which is the crime of account breaches through digital banking services. This crime, involving the illegal exploitation of digital system loopholes to access consumer funds, has caused substantial financial losses (Evenett & Jenny, 2000).

These cases of digital account tampering are of serious concern, especially in relation to the protection of consumer protections. Many victims of digital account breach find it difficult to obtain legal compliance and justice, due to the absence of clear provisions regarding the responsibility of banks and service providers in this regard. Although banks often try to prioritize strict security systems, in reality, many consumers become victims due to negligence or gaps in the existing security system. This requires clear legal provisions to ensure who is responsible when a crime occurs (Devanto, 2017).

Existing regulations are often considered insufficient to provide maximum protection to consumers. Law Number 8 Year 1999 on Consumer Protection and Law Number 21 Year 2011 on the OJK provide the legal basis for consumer protection and supervision of financial institutions, but unclear implementation and indecisiveness in dealing with digital crime cases can cause uncertainty for consumers. The division of responsibility between banks and consumers in addressing data leaks and account tampering remains an evolving issue that requires special attention (Ramasari, 2016).

* *Corresponding author, email address:* ***dr.yenivitrianingsih@gmail.com***

Digital account tampering also highlight the importance of transparency in the operation of digital banking security systems. Consumer data protection, which is one of the most important parts of banking services, is often overlooked or not clearly communicated to consumers (Medita, 2014). Non-transparent processes and lack of consumer understanding of potential risks can make matters worse when a breach occurs. To realize a safer and fairer banking system, concerted efforts are needed to ensure security and clarity of legal for the consumers who become victims of crime (Dharma, 2012).

One of the main problems in cases of account tampering through digital banking services is the lack of clarity about who is responsible in the event of a crime. The Consumer Protection Law provides certain rights to consumers, but in reality, there is often no clarity on the procedures that consumers must take to obtain compensation or settlement in the event of an account tampering (Harry, 2015). This leads to legal uncertainties that are detrimental to consumers, especially for those who do not have sufficient understanding of their rights in digital transactions. Clarity in this regard is very important to maintain consumer satisfaction with banking institutions (Kuncoro, 2013).

Although The Central Bank of Indonesia (BI) and the OJK have regulated various policies to protect consumers from cybercrimes, practice on the ground shows that the implementation of these policies is often inconsistent. For example, large banks have more sophisticated protection systems, however, smaller banks or other financial institutions may not fully comply with the same security standards. This leads to disparities in the level of protection provided to consumers. Stricter regulations and more effective supervision from authorities are needed to ensure all banking institutions adhere to the same standards.

Finally, consumer education and understanding of digital banking security is also a significant issue. Many consumers still lack an understanding of the risks and appropriate means of protection when using digital banking services. While efforts to promote secure digital banking, many consumers neglect precautions like strong passwords, two-factor authentication, and transaction monitoring. This opens up opportunities for criminals to exploit consumers' negligence and take advantage of their ignorance to commit crimes.

The importance of legal certainty in cases of digital account tampering cannot be underestimated. This growing cybercrime not only harms individual consumers, but can also damage the image of the banking system itself. In the long-term, legal uncertainty can reduce the level of public trust in digital banking services, which in turn can affect the development of the digital financial sector. It is important to conduct a research and analysis of the supervision mechanism and the application of existing legal sanctions so that consumer protection can be guaranteed more optimally.

This research aims to analyze the legal certainty provided to consumers in the face of account tampering through digital banking services. This research will also explore how existing supervision mechanisms, as well as the application of applicable sanctions, can provide maximum protection for consumers in the face of cybercrime risks. The results of this research are expected to contribute to formulating better policies and a more effective supervision system, so that public trust in digital banking services can be well maintained.

RESEARCH METHOD

This research uses a literature research approach with a normative juridical method to analyze legal compliance in cases of digital account tampering crimes. This approach focuses on analyzing applicable laws and regulations, court decisions, and literature relevant to the research topic. The literature research was conducted by reviewing various primary and secondary legal sources related to a consumer protection issue in the digital banking system. Primary legal sources used include legislation such as Law Number 8 Year 1999 on Consumer Protection and Law Number 21 Year 2011 on the OJK, as well as BI regulations governing the operation of electronic payment systems. This research also refers to official documents and related reports from authorized institutions, such as OJK and BI. This normative approach examines how effectively current regulations protect consumers from digital account tampering.

In the normative juridical approach, this research will analyze legal provisions by comparing various regulations related to supervision and law enforcement in the industrial sector involving digitalization, as well as how existing arrangements are applied in practice (Negara & Darmawan, 2023). References used include scientific works from legal experts that discuss consumer protection issues in the digital era, such as the book Legal Research Methodology by Soekanto (2015), which reviews in detail the ways to conduct juridical analysis in legal research. With this approach, it is hoped that a better solution can be found related to legal compliance in digital banking supervision, as well as the application of sanctions that can provide maximum protection for consumers. Literature from sources such as Consumer Protection Law by Kadir (2017)

will also be used as the main reference in analyzing existing policies, as well as to see the extent of successful implementation of existing regulations in mitigating the risk of cybercrime.

RESULT AND DISCUSSION

Rapid developments in information technology, particularly in the digital banking sector, have brought significant impacts to the way people interact with financial services (Azharuddin, 2019). The use of mobile banking applications, digital payments, and online transaction systems enables tremendous convenience in daily economic activities. With all this convenience also comes a great risk in the form of increasingly sophisticated cybercrime threats, which can harm individuals and society as a whole. These increasingly prevalent crimes, such as account tampering through digital banking services, show that while technology provides many advantages, it also opens up loopholes for criminals to exploit weaknesses.

Digital account tampering has a clear example of cybercrime that utilizes technological advances to steal consumer funds. In this mode, perpetrators use various methods, such as phishing, malware, and attacks on digital banking protection systems, to gain illegal access to consumer accounts. As a result, consumer funds can disappear without a trace, and consumers are often faced with huge financial losses. These crimes are growing in line with society's increasing reliance on digital banking services, which demands stricter protection systems and clear legal protections (Kuncoro, 2013).

In the face of this phenomenon, legal compliance is a very crucial aspect. Consumers need assurance that their rights are firmly protected, and that they can obtain compensation or a fair legal settlement if they become victims of cybercrime. It is known that the agreement between consumers and banks is generally in the form of a standard agreement, which often puts consumers in a position where their rights are minimized. A standard agreement is an agreement that binds all parties who sign it, even though there are clauses that often shift the burden of responsibility from the party who drafted the agreement to the opposing party. Any losses that arise in the future remain the responsibility of the parties involved, in accordance with the provisions in the agreement clause, unless the clause violates the provisions stipulated in Article 18 of the Consumer Protection Law.

A standard agreement is drafted in advance by one of the parties, usually a manufacturer or financial institution, and then signed by the consumer who has no other choice. All provisions contained in the agreement will be binding on both parties. Important to note that the content of the agreement must be in accordance with applicable laws and regulations, including the provisions prohibited in Article 18 of the Consumer Protection Law. This shows that a good understanding of the standard agreement is essential for consumers to be aware of the rights and obligations stipulated in the agreement. It is important to ensure that existing regulations can provide maximum protection and establish clear mechanisms regarding the responsibilities of related parties, be it banking institutions, digital service providers, or criminals. Stricter supervision and effective application of the law are needed so that the crime of account breach through digital banking services does not further harm consumers and create uncertainty in the world of digital banking.

Legal compliance in dealing with digital account tampering cases in Indonesia is closely related to the implementation of various regulations governing the banking system and personal data protection. One of the main regulations governing this matter is Law Number 11 Year 2008 on Electronic Information and Transactions (ITE), which was later updated with Law Number 19 Year 2016 on the amendment of ITE Law. This ITE Law provides the legal basis for tackling cybercrime, including those related to the breach of banking accounts through the intermediary of digital platforms. While these regulations, in practice, the implementation of the law against cybercriminals still faces various obstacles, one of which is in terms of evidence that must be submitted in court to prove the crime.

The importance of legal compliance in this case is related to the protection of consumers from a legal perspective, and also from the aspect of recovering losses suffered by consumers due to account tampering. As the number of cases involving digital banking services increases, the question arises as to who should be held liable in such cases: the bank, the digital technology service provider, or the consumer himself (Wafiya, 2012). In some cases, consumers feel aggrieved that banks are not able to protect their data and transactions well enough. For example, if the bank does not provide an adequate authentication system or does not act promptly after noticing suspicious activity, the consumer has the right to claim damages in accordance with applicable laws.

The supervision mechanism for digital banking services in Indonesia is specifically carried out by the OJK, which works to ensure that financial services institutions, including banks, comply with operational standards that are safe for customers. OJK has issued regulations regarding the implementation of security systems in digital transactions, which include the obligation of banks to use strong encryption systems,

as well as policies that pay attention to the protection of consumer personal data (Medita, 2014). BI also has policies related to electronic payment systems that must be implemented by banking institutions to avoid cybercrime. This supervision still faces obstacles in terms of uniform implementation across financial institutions, as well as challenges in dealing with increasingly complex cybercrime.

In terms of sanctions, the ITE Law has regulated the penalties for cybercrimes, including those related to digital account tampering. Article 30 of the ITE Law regulates the prohibition of illegal access to electronic systems, which can lead to imprisonment and fines for perpetrators. This sanction is more focused on the individual committing the offense, while in practice, account tampering cases often involve third parties collaborating with outside parties, making it difficult to provide effective sanctions for all parties involved. It is important to pay attention to the recovery aspect of aggrieved consumers, where currently, there is no clear mechanism regarding the process of compensation or responsibility from the bank to the victimized customer.

An effective supervision process requires better collaboration between various related parties, such as OJK, BI, law enforcement agencies, and the banks themselves. Without proper coordination, oversight of digital account tampering may be slow and ineffective in curbing cybercrimes in banking. It is expected that there will be efforts to strengthen the supervision system through the use of advanced technology, such as artificial intelligence to detect suspicious transactions more effectively and quickly. Devanto (2017) noted this system can be a better preventive measure to prevent large losses for consumers and ensure the protection of the digital banking system in Indonesia.

According to legal compliance, it is very important to ensure that there are clear and firm regulations that can provide protection for consumers who are victims of account tampering (Setiadi, 2017). This includes clarifying the roles of each party involved in digital banking services. Bank service providers should be responsible for ensuring that the systems they offer are secure and not vulnerable to cybercrimes, while consumers should also be educated on how to protect their personal data (Medita, 2014). With more detailed regulations and firmer legal mechanisms, it will be easier for consumers to obtain justice when facing the problem of digital account tampering (Rildayanti, 2014).

At the international level, Indonesia can also look at the practices implemented by other countries in dealing with digital banking crime cases. Some developed countries have implemented stricter laws related to digital account tampering, as well as created independent supervision bodies specialized in handling cybercrime in the banking sector (Ramasari, 2016). By researching these best practices, Indonesia can adjust its policies and supervision mechanisms to better suit the evolving dynamics of digital banking. This will improve Indonesia's ability to handle similar cases in the future more effectively and efficiently.

Legal compliance must also include the consumer's rights to obtain fair compensation in the event of a loss due to digital account tampering. Without clarity in this regard, consumers may feel aggrieved and lose trust in the rapidly growing digital banking system (Dharma, 2012).

In the event of losses suffered by consumers using internet banking services, it is important to examine the responsibilities of the parties involved in the service. The main question that needs to be answered is who is responsible for the losses suffered by the consumer, whether it is the bank, the consumer himself, or another party. Based on the standard agreement between the consumer and the bank, it appears that the bank is not liable for any loss suffered by the consumer in the use of internet banking services, especially if the loss is related to privacy or material loss.

From the perspective of applicable statutory provisions, privacy or material losses experienced by consumers are more related to legal protection. Legal protection can be divided into two types, namely preventive legal protection and repressive legal protection. Preventive legal protection aims to prevent disputes, while repressive legal protection aims to resolve disputes that have occurred.

In this case, preventive legal protection for consumers in internet banking transactions includes prevention efforts that are part of internal banking policies, such as supervision and guidance of commercial banks in carrying out electronic transactions. Meanwhile, repressive legal protection is carried out by applying sanctions against perpetrators who violate the provisions, with the aim of restoring the legal situation to its proper position. An understanding of the responsibilities and legal protection in internet banking services is very important to protect the rights of consumers.

Law Number 21 Year 2011 on the OJK emphasizes the importance of consumer and community protection in the financial services sector. OJK has the authority to take preventive measures against losses experienced by consumers and the public, as well as provide information and education on the characteristics of the financial services sector,

services, and products available. This research in the law indicates that consumer education is necessary to support the legal protection of consumer data in internet banking services. This provision does not explicitly stipulate the responsibility of the bank in the event of material loss suffered by the consumer.

The Central Bank of Indonesia Regulation Number 7/7/PBI/2005 on Customer Complaint Settlement, as amended by The Central Bank of Indonesia Regulation Number 10/10/PBI/2008, regulates the substance of consumer complaint settlement. In this provision, BI requires all banks to resolve any consumer complaints related to financial losses experienced. This regulation also regulates the procedures for receiving, handling, and monitoring the settlement of consumer complaints. Banks are required to provide quarterly reports to BI regarding the implementation of the settlement of consumer complaints. This regulation aims to improve accountability and transparency in the settlement of consumer complaints in the banking sector.

The OJK regulation stipulates that banks must apply the principles of controlling and securing consumer data and transactions in electronic banking services on every electronic system used. In Article 21, it is emphasized that banks that organize electronic banking services or digital banking services must apply consumer protection principles in accordance with the provisions of laws and regulations applicable in the financial services sector.

If the internet banking organizer, in this case the bank, does not comply with these provisions, it will be subject to administrative sanctions. These sanctions can be in the form of a written warning, a decrease in the bank's health level as reflected in the governance factor rating, a prohibition to issue new products or carry out new activities, as well as the suspension of certain businesses. Ineligible members of the board of directors, board of commissioners, and executive officers can be included in the list of not passing through the fit and proper test mechanism. This regulation aims to ensure that banks are responsible for protecting consumer data and transactions and complying with consumer protection principles.

From the perspective of Law Number 11 Year 2008 on Electronic Information and Transactions, there is no research that specifically regulates internet banking. There is an article that regulates transactions through internet media, namely Article 9, which states that "Business actors offering products through electronic systems must provide complete and correct information relating to contract terms, producers, and products offered."

Overall, the protection of consumers using internet banking services provided by banks in terms of technological security is considered adequate. This is due to the fact that some banks have implemented internet banking transactions, including the protection provided through the use of PIN tokens. This provision only regulates the legal protection of consumers from a preventive and repressive perspective, without emphasizing clear aspects of legal liability.

The question that arises is whether there is no regulation on material liability suffered by consumers in Indonesian legislation. It is important to further explore the legal liability aspects of internet banking services so that consumers can be comprehensively protected.

Explicitly, there is no detailed regulation regarding the bank's liability for privacy or material losses suffered by consumers. When referring to Article 21 Paragraphs 2-4 of Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions, there is a legal basis that regulates liability in the implementation of internet banking. Article 21 Paragraphs 2 to 4 states that: 1) The party responsible for all legal consequences in the implementation of electronic transactions is regulated as follows: a) If the transaction is conducted alone, all legal consequences shall be the responsibility of the parties to the transaction; b) If the transaction is conducted through the granting of power of attorney, all legal consequences shall be the responsibility of the grantor of the power of attorney; and c) If the transaction is conducted through an electronic agent, all legal consequences shall be the responsibility of the electronic agent organizer.

If the loss in an electronic transaction is caused by the failure of the electronic agent to operate due to the actions of third parties that directly affect the electronic system, then all legal consequences are the responsibility of the electronic agent organizer. If the loss is caused by the negligence of the service user, then all legal consequences are the responsibility of the service user. From these provisions, it can be concluded that the burden of responsibility depends on the fault of the parties involved in the transaction.

Laws and regulations are more likely to require banks, as producers, to strengthen their systems and provide explanations regarding risks that may arise to consumers. If in the future there is an event that harms the consumer, the burden of responsibility should not be shifted to the bank.

In the condition of losses caused by external parties, such as cybercrime perpetrators, the regulation regarding this matter has been regulated in Article 27 of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

The research states that "Every person intentionally and without right distributes and/or transmits and/or makes accessible electronic information that has content that violates decency." Article 30 of the ITE Law also emphasizes several provisions, including: 1) Any person who intentionally and without rights or unlawfully accesses another person's computer and/or electronic system in any way; 2) Any person who intentionally and without rights or unlawfully accesses a computer and/or electronic system with the purpose of obtaining electronic information and/or electronic documents; and 3) Any person who intentionally and without rights or unlawfully accesses a computer and/or electronic system in any way that violates, breaks through, exceeds, or breaches the security system.

These researchs outline several crimes in Law Number 11 Year 2008 on ITE, which functions as a lex specialis of the Criminal Code (KUHP). This law aims to complement the provisions in the KUHP, so that if an act is not regulated in the KUHP, then this law can be applied. Destructive actions by external parties that result in losses target consumers, and the bank itself. To suffering material losses, banks are also at risk of getting a bad image in the community, which can reduce public confidence in their ability to manage and distribute public funds.

Overall, it can be concluded that in the perspective of crime law, liability for losses suffered by consumers in the use of internet banking services is still based on the concept of fault of the parties involved. Error is defined as culpa, which in relation to the law has a technical meaning as a form of crime perpetrator error that is not as serious as intentionality, namely a lack of caution that results in unintended consequences. Negligence on the one hand contrasts with intentionality and on the other hand with coincidence. In the study of criminal law, there are two kinds of fault: willfulness and negligence. In the research of crime law, there are two kinds of fault: intentionality and negligence. The difference between the two lies in the offender's awareness of the results or consequences of his actions. Willfulness has a more negative moral value than negligence, because the intentional act is intended to realize the prohibited result.

According to civil law, fault is also included in the elements of tort. This unlawful act is regulated in Article 1365 of the Civil Code of Indonesia, which states that "Every unlawful act that causes damage to another person, obliges the person whose fault caused the damage to compensate for the damage." In both criminal and civil law, fault is an important element in determining liability for losses suffered.

Unlawful acts are deemed to occur when there is an action of the perpetrator that violates the law, contradicts the rights of others, violates the perpetrator's legal obligations, contradicts decency and public order, or is not in accordance with the norms of decency in society, either against themselves or others. Nevertheless, an unlawful act must still be accountable, including whether or not the act contains elements of fault.

Article 1365 of the Civil Code of Indonesia does not distinguish between intentional fault (opzet-dolus) and negligent fault (culpa). Judges must be able to assess and consider the severity of the wrongdoing committed by a person in relation to unlawful acts, so that fair compensation can be determined. If the element of fault in an act can be proven, then the perpetrator is responsible for the harm caused by the act. A person can also be liable for losses caused by the fault of his dependents, goods under his supervision, and pets, as stipulated in Article 1366 to Article 1369 of the Civil Code of Indonesia.

Unlawful acts regulated in Article 1365 of the Civil Code of Indonesia can be used as a basis for claiming compensation for acts that are considered unlawful in the process of online business transactions. The occurrence of unlawful acts in online business transactions that cause losses requires rules that become the legal basis for compensation claims. The Civil code of Indonesia and the ITE Law have an important role, because legally, online transactions have not been regulated in Indonesian legislation. In accordance with the mandate of the Judicial Power Act, judges are required to explore the values that live in society so that there is no legal vacuum, so judges cannot reject cases that enter the court on the grounds that there are no or incomplete rules.

Extensive legal interpretation, which expands the meaning of words in a statute, is one way to overcome this problem. Article 1365 can be used as a legal basis for compensation claims for unlawful acts in internet banking transactions, with evidentiary support based on electronic data recognized as valid evidence, as stipulated in Article 5 of the ITE Law.

The regulation regarding the compensation mechanism must be set forth in a special law or regulation so that consumers can obtain justice without going through a long and convoluted legal process. Legal remedies in dispute resolution can be pursued in two ways: first, out of court. Consumers can sue the bank out of court through an institution known as the Consumer Dispute Resolution Agency (BPSK). BPSK is a special institution established by the government in each level II region to resolve disputes outside the court. In accordance with BI regulations,

there is also an independent institution known as the Indonesian Banking Dispute Resolution Alternative Institution (LAPSPI), which is formed by banking associations and registered with the OJK. Just like BPSK, LAPSPI provides three dispute resolution services, namely mediation, adjudication and arbitration.

Second, the court route. The use of this route is generally the last step after mediation efforts between the parties. Dispute resolution procedures in court will be adjusted to the applicable civil procedural law. Dispute resolution procedures in court will be adjusted to the applicable civil procedural law, which includes steps such as filing a lawsuit, examining evidence, and trial. In this process, the judge will listen to the arguments of both parties, assess the evidence submitted, and finally decide the case based on the applicable legal provisions.

A consumer has the right to adequate legal protection. This protection is important to give customers a sense of security and confidence that their rights are respected and protected in accordance with applicable legal provisions. Without clear protections, customers risk losses that are difficult to recover, especially in cases involving data misuse or fraud. Both out-of-court and court channels must provide fair and transparent access for consumers to claim their rights.

With these various dispute resolution mechanisms, it is expected that consumers can obtain justice efficiently and effectively, without having to be trapped in a long and complicated legal process. This is important so that customers still feel protected and not burdened by convoluted procedures, so that their rights can be fulfilled more easily. A clear regulation of liability and compensation mechanisms in internet banking transactions will provide legal certainty for all parties involved, and increase public confidence in digital banking services.

Overall, the development of comprehensive regulations and effective dispute resolution mechanisms is critical to creating a safe and secure environment for consumers to use internet banking services. This will protect the rights of consumers, and contribute to the stability and integrity of the financial system as a whole.

To achieve maximum protection for consumers, Indonesia needs to take concrete steps in strengthening supervision and law enforcement related to digital account fraud. This can be achieved through the improvement and development of a more sophisticated and up-to-date digital banking security system, so that it can anticipate all forms of cyber threats that continue to evolve. Better system security will reduce opportunities for criminals, and increase public trust in digital banking services (Harry, 2015).

More effective coordination between relevant institutions, such as BI, the OJK, and the police, needs to be strengthened so that law enforcement against cybercrime perpetrators can run more efficiently and on target. Integrated supervision will enable faster and more precise handling of cases of account tampering that harm consumers. Moreover, existing regulations must also be adjusted to technological developments to create a more comprehensive legal framework for safeguarding consumers' personal data and transactions (Effendi, 2020).

With more coordinated efforts and a justice system that is responsive to the development of cybercrime, it is hoped that the public will feel safer in utilizing digital banking technology. Firm and fair law enforcement will provide a deterrent effect for criminals and encourage the banking sector to continue to innovate in creating safe solutions for consumers. Ultimately, the ultimate goal is to create a digital banking ecosystem that prioritizes convenience and accessibility, and provides a sense of security for all users.

CONCLUSION

Legal certainty in dealing with cases of account tampering through digital banking services in Indonesia still faces significant challenges, while the existence of regulations governing this matter, such as the ITE Law and regulations related to personal data protection. Although supervisory efforts by the OJK and bi are in place, their implementation is still not fully optimized. This can be seen from the many cases of account breaches that have not received adequate resolution. For this reason, strengthening coordination between related institutions and improving digital transaction security systems are inevitable. With the development of digital technology, it is expected that the digital banking system can be safer and more guaranteed protection for consumers.

The implication of this finding is the importance of improving the current supervision mechanism, especially by strengthening the capacity of supervisory institutions and implementing more sophisticated security technology in the digital banking system. There needs to be further efforts to clarify the legal responsibilities of the parties involved, be it banks, technology service providers, or the consumers themselves. In this case, there needs to be legal clarity regarding the sanctions that can be given to parties who are negligent or involved in cases of account tampering, as well as the rights of aggrieved customers to obtain fair compensation.

Suggestions that can be made are the importance of revising or strengthening regulations related to cybercrime that leads to digital account tampering.

The implementation of more sophisticated security technology and stricter authentication procedures is also highly recommended to reduce the loopholes that can be utilized by criminals. Supervisory institutions need to strengthen supervision more comprehensively and prioritize transparency in handling every case of cybercrime in the banking sector. Educating the public on ways to protect personal data and the obligation for banks to provide maximum protection are important steps in reducing consumer losses.

REFERENCES

Azharuddin, A. (2019). Legal Protection for Users of Internet Banking Consumers Following Changes in Information and Electronic Transactions Law. *Journal of Law*, 6(1), 67-78.

Dandash, O., Le, P. D., & Srinivasan, B. (2007). Security Analysis for Internet Banking Models. *In Conference: Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 3, 1141-1146.

Devanto, S. P. (2017). Perlindungan Hukum Nasabah dalam Transaksi melalui Internet Banking. *Indonesian Journal of Legal Studies*, 10(3), 201-218.

Dharma, S. (2012). Perlindungan Hukum bagi Konsumen Internet Banking (Studi pada E-Banking Bank Mandiri). *Journal of Consumer Law*, 9(2), 67-85.

Effendi, B. (2020). Pengawasan dan Penegakan Hukum terhadap Bisnis Digital (E-Commerce) oleh Komisi Pengawas Persaingan Usaha (KPPU) dalam Praktek Persaingan Usaha Tidak Sehat. *Syiah Kuala Law Journal*, 4(1), 21-32.

Evenett, S. J., & Jenny, F. (2000). *Competition Law and Economic Integration in Developing Countries*. Edward Elgar Publishing.

Harry, N. P. (2015). Perlindungan Hukum terhadap Nasabah Pengguna Fasilitas Internet Banking atas Terjadinya Cyber Crime. *Journal of Law Protection*, 45(3), 142-156.

Kadir, A. (2017). *Hukum Perlindungan Konsumen*. Sinar Grafika.

Kuncoro, T. (2013). Penegakan Hukum terhadap Cyber Crime di Bidang Perbankan. *Journal of Legal Studies*, 11(2), 75-85.

Medita, R. (2014). Perlindungan Hukum bagi Nasabah terhadap Keamanan Data Pribadi Nasabah dalam Layanan Internet Banking. *Journal of Legal Protection*, 45(3), 142-156.

Negara, D. S., & Darmawan, D. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13-19.

Bank Indonesia. (2016). *Peraturan Bank Indonesia Nomor 18/40/PBI/2016 Tahun 2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.* Lembaran Negara Republik Negara Nomor 236 Tahun 2016. Jakarta.

Otoritas Jasa Keuangan. (2016). *Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 Tahun 2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.* Lembaran Negara Republik Indonesia Nomor 324 Tahun 2016. Jakarta.

Ramasari, R. D. (2016). Legal Protection of Bank Consumers in Cyber Crime Connected with the Internet Banking Law. *Journal of Cyber Law*, 5(2), 153-160.

Rildayanti, M. (2014). Perlindungan Hukum bagi Nasabah terhadap Keamanan Data Pribadi dalam Layanan Internet Banking. *Journal of Legal Protection*, 45(3), 142-156.

Setiadi, T. (2017). Perlindungan Hukum terhadap Nasabah yang Mengalami Kerugian dalam Penggunaan Internet Banking yang Disebabkan oleh Intervensi Pihak Lain. *Journal of Law Studies*, 35(1), 103-118.

Soekanto, S. (2015). *Metodologi Penelitian Hukum*. Rajawali Pers.

Republik Indonesia. (2016). *Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Nomor 251 Tahun 2016. Tambahan Lembaran Negara Nomor 5952. Sekretariat Negara, Jakarta.

Republik Indonesia. (2011). *Undang-undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.* Lembaran Negara Republik Indonesia Nomor 111 Tahun 2011. Tambahan Lembaran Negara Nomor 5253.

Republik Indonesia. (1999). *Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.* Lembaran Negara Republik Indonesia Nomor 22 Tahun 1999. Tambahan Lembaran Negara Nomor 3821. Sekretariat Negara, Jakarta.

Wafiya, W. (2012). Perlindungan Hukum Bagi Nasabah yang Mengalami Kerugian dalam Transaksi Perbankan Melalui Internet. *Journal of Legal Studies*, 14(1), 37-52.

***Fitrotinisak, I. K., R. Mardikaningsih, E. C. Gautama, S. Sulani, Y. Vitrianingsih. (2023). Legal Compliance for Consumers in Dealing with Cases of Account Tampering in Digital Banking Services, *Journal of Social Science Studies*, 3(1), 75 – 82.**