Rechtsregel
Jurnal Ilmu Hukum
Vol 8, No. 2 Desember| 2025
P-ISSN 2622-6235, E-ISSN 2622-6243
rjih_fh@unpam.ac.id

CYBER SECURITY REACUALIZATION OF CUSTOMER DATA AND FUNDS IN THE OPTICS OF ELECTRONIC INFORMATION AND TRANSACTIONS

Taufik Kurrohman [1] Fenny Wulandari [2]
Fakultas Hukum Universitas Pamulang
Email : [1]dosen00643@unpam.ac.id, [2]dosen01493@unpam.ac.id

ABSTRACT
The technological transformation in the digital era has changed the paradigm of the banking world. Financial access is now inseparable from space, distance, and time, as it only requires the internet and sophisticated devices for every customer to make transactions. On the other hand, cyber security of customer data and funds is very risky to be hacked with various instruments and methods such as fishing, spam, ransomware to cause material losses, historically cyber attacks have been experienced by Bank Indonesia on January 21, 2022, Bank BSI May 2023 and most recently Bank BRI on December 18, 2024, but not transparently impacting customers. Customer protection is based on the regulation of Law Number 1 of 2024 concerning Electronic Information and Transactions and does not specifically regulate the protection of customer data and funds. The purpose of the research focuses on the practical order of cyber regulation in protecting customer data and funds, and the reactualization of the provisions of laws and regulations. The research method was carried out with normative juridical analysis with qualitative normative data analysis. The results of the study show first, the actual condition of cyber security today through the provisions of the ITE law has not been carried out comprehensively verified in the context of law enforcement the evidentiary instruments are inadequate, the jurisdiction of the authority limits the accessibility of cyber security law enforcement, there has been no case of buying and selling bank customer data that has been punished in the second court, the reactualization of cyber security data and funds can be carried out by strengthening the evidentiary instruments for Law Enforcement, Interpol cooperation between countries specifically for cybersecurity.

Keywords*: reactualization; cybersecurity; data and funds; bank.*

PENDAHULUAN

The technological transformation in Indonesia today has changed the paradigm and culture in society, including banking transaction methods. Now, customers can perform transactions without space and time limitations, only requiring an internet connection and advanced devices to conduct transactions (Prahassacitta, Vidya, 2023).

The latest data released by the Indonesian Internet Service Providers Association (APJII) in 2024 recorded that internet users in Indonesia reached 221,563,479 people. This fact shows an increase of 1.4% from the previous figure, with the total population of internet users reaching 79.5%. Specifically for mobile banking usage in Indonesia, data from 2024 shows good growth in both transaction volume and users, with details in the following table: (diakses tanggal 09 Mei 2025)

Bank	User	Previous Period	Growth
Bank Rakyat Indonesia	33,5 Million	25,7 Million	30,3% YOY

Bank Central Asia	30,8 Million	28,3 Million	9% YOY
Bank Mandiri	24 Million	-	39 % YOY
Bank Negara Indonesia	16,9 Million	14,3 Millions	18,5 YOY
Bank Syariah Indonesia	7,57 Million	-	28,34 YOY

Table I Mobile Banking User Data Quarter 1 Year 2024
Source: summarized by the author from various sources

Suspected to have been affected by a cyber attack that resulted in inaccessibility to banking services, leakage of customer personal data, and loss of customer funds. Facing the cyber attack, Bank Syariah Indonesia has made preventive efforts by increasing the IT security budget to strengthen the security system. Secondly, PT. Bank Rakyat Indonesia, dated December 18, 2024, disclosed by Falcon Feeds has warned of the potential ransomware attack on the bank, although this has been clarified by BRI Bank stating that the security system meets international standards and banking services are running smoothly without any issues. Third, Bank Central Asia provides information that throughout 2024, it has experienced 4 billion cyberattacks, which previously recorded 1.9 billion cyberattacks. Data indicates that cyberattacks from year to year are increasing, often in the form of DDoS (Distributed Denial of Service), where authorized customers cannot access bank services (diakses tanggal 08 Mei 2025)

Based on these facts and data, it is important to mitigate the risk of banking system hacking, because banks operate based on the principles of trust. The security of customer data and funds is an important part to be guaranteed in preventing the negative effects of technological developments with the aim of national economic growth (Destyarini, Normalita. 2024: 218-233). Omekanye et al. concluded in their research that financial crime preventive measures that have been transformed are based on artificial intelligence, cybersecurity performance, data sophistication with high-tech capabilities that must be carried out synergistically with data privacy, regulation and implementation (Omokanye, Abraham Okandeji, et al, 2024). The urgency of know your customer principles is not only applied to regular customers but also to customers who access mobile banking (Fadia, Yanti, and Muhammad Alwan Zain Nusantara, 2023: 252-269).

The urgency of know your customer principles is not only applied to regular customers but also to customers who access mobile banking. The data above is the smallest part of the use of the latest technology, especially in the banking world. Seeing the actual condition of cyber security of customer data and deposits as a preventive measure and legal protection for customers, in this context is an important part that intersects with consumer protection. Customers and personal data, and funds that must be protected with qualified security, both from the regulatory aspect and from the protection aspect in the practical order.

Consumer interpretation based on the provisions of the Consumer Protection Act focuses on goods and/or services that exist in the community, both in the context of personal interests and others. Rights that must be protected are reflected in the protection of comfort, safety and safety in the consumption of goods and services. (Destyarini, Normalita. 2024: 218-233). Banks as an intermediary institution that connects those who have money with those who need money and are based on trust values must have strong power to protect the interests of consumers, especially in the data and funds entrusted to banks.

In the practical order, it is not so easy to actualize and interpret in a practical order whether data hacking, buying and selling data on the black market and data loss are unlawful acts committed by banks or are negligence from consumers. An act is said to be unlawful if it is indicated to cause concrete and verifiable harm, in the case of the case mentioned above, to be categorized as a violation or negligence, at least the following must be verified: first, there is a positive or negative act, both acts are categorized as unlawful acts, third, indications of loss, fourth, there is causality between the act and violating law and fifth, the existence of an error (Destyarini,

Normalita. 2024: 218-233) From several cases that have occurred, the practical order of actualizing the ITE law in cyber law enforcement is important to be evaluated on an ongoing basis.

Continuous evaluation of the implementation of cybersecurity, especially banking, is considered important to be carried out, this effort is by reactualizing the application of the law in the law enforcement process. Periodically in the context of laws and regulations, there are no special provisions, but based on the provisions of Article 1 number 14 concerning the formation of laws and regulations, it is known as monitoring and review. These efforts are carried out as a benchmark and achievement of the implementation of laws and regulations since they were enacted, both benefits and harms and the accompanying impacts (Aris, Mohammad Syaiful, and Dita Elvia Kusuma Putri : 2024).

The acceleration of technology and information has both good and bad impacts, like a double-edged sword because there is a space that gives a person a gap to do what is detrimental to others, such as data theft and sales on the black market. Data exchange can now be done with web-based platforms and applications, for example, by listing data according to personal identity, name, date of birth, work address, population identification number and other personal data. In this condition, data becomes a commodity and becomes a valuable asset and can be traded and has the potential for data misuse (Mentari, Nikmah, Ninis Nugraheni, and Muhammad Annas, 2023)

Are the latest regulations sufficient to make preventive efforts to protect the security of customer data and funds? Bank Indonesia has the authority to provide regulations through the Bank Indonesia Regulation (PBI) with digital payment systems and technology-based financial transactions, as well as the Financial Services Authority (OJK) which supervises technology services through OJK regulations (POJK) on aspects of technology-based lending and digital financial innovation. These regulations have not had a direct impact in terms of consumer protection related to customer data and funds (Durianto, Darmadi, et al: 41.1: 19-30)

Data privacy is very closely related to the effectiveness of legal regulations, which can be seen by resolving cross-border issues related to data. Obstacles are faced because management by global companies has not been protected by the provisions of existing laws and regulations. (Arbani, Tri Suhendra, and Aulia Hasanah Putri. 13.3: 2024) The security of customer data and funds must be interpreted comprehensively in an effort to handle law enforcement both preventively and repressively. The provisions of the ITE Law represent the current condition in efforts to handle data security that has not been fully realized. Cyber hacking data that cannot be found and punished before the court is one of the benchmarks for the success of data security in the context of the implementation of the Information and Electronic Transactions law.

RESEARCH PROBLEMS

First, How the Actual Conditions of Cyber Security in Protecting Customer Funds and Data in Electronic Transactions and Second how is the Reactualization Strategy to Improve Cyber Security of Banking Customer Data and Funds

RESEARCH METHODS

The research method is based on primary and secondary data with normative and stable juridical approaches. Statutorial is an approach with a review methodology from various points of view of laws and regulations that are substantially relevant to the object of the problem being discussed. (Muhammad, Abdulkadir, 2004) Data collection through the latest literature from journals, books, the internet and laws and regulations whose focus is substantially on the security of bank customer data and funds as well as electronic information and transactions. The data is analyzed qualitatively with relevant theories. This paper seeks to describe the current state of data and fund security in banks in relation to the actual conditions of cyber security mitigation and the

implementation of regulations. The transparency of losses caused by cyber attacks on banks is perceived only as public consumption in the media, without accurate clarity on whether it harms customers materially.

RESULT AND DISCUSSION

Actual Conditions of Cyber Security in Protecting Customer Funds and Data in Electronic Transactions

Cybersecurity, especially in the banking world, is important because banks run based on public trust. If trust is lost with the vulnerable cause of cyber attacks and weak data security, then this becomes a setback for banking. Consumer protection is a top priority for the creation of guarantees that have an impact on public trust for economic development nationally.

Based on the theory of a welfare state based on the values of Pancasila and the 1945 Constitution of the Republic of Indonesia on the practical order of consumer protection is one of the goals of justice that can provide legal certainty, businessmen contribute to inherent responsibility, and the impact of providing awareness to consumers (Nofrial, Ramon, et al. 41.1: 73-91). Customer data protection has become a necessity to mitigate in accordance with current regulatory provisions. The implementation carried out by banks is by using encryption and dual authentication to secure customer data, but unfortunately, encryption and authentication do not automatically function as they should, as it requires the involvement of consumers to do so. This shows that consumer awareness is also important to be enlightened. Risk analysis of data confidentiality and security is conducted by banks in institutional collaboration to provide security and comfort to customers. Example: one of the regional development banks (BUMD) during the Eid holiday in 2025 could not execute transfers to other banks, which were supposed to be available via the mobile banking menu. On television and other media, it was verified with an explanation from one of the authorized officials at the bank that this was done to automatically protect the system in case of suspected system irregularities or hacking. This incident had a negative impact on the bank as it had to lose many of its loyal customers.

The Bank has the obligation to provide clear and accurate information and transparency to customers in terms of collecting customer personal data and provide complaint instruments that are easily accessible in an effort to handle indications of privacy violations. 24-hour service for example in the event of complaints, deletion of data when not needed, withdrawal of consent and other relevant policies.

Article 1 paragraph 5 of Law Number 11 of 2008 concerning Information and Electronic Transactions states:

> " Electronic Systems are a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate Electronic Information"

Article 1, paragraph 8:

> "An Electronic Agent is a device of an Electronic System that is designed to perform actions on certain Electronic Information automatically and is organized by a person".

Algorithms that have been developed by banks or electronic agents through certain applications and websites give banks the responsibility to protect the security of customer data. Through the procedures that have been set, the bank provides clarity and certainty to customers that all data provided is guaranteed by the bank, and for bank actions that may result in the dissemination of customer data and loan funds, it can be prosecuted for unlawful acts that result

either directly or indirectly to customers. The phrase electronic agent can be interpreted as an institution that attaches rights and obligations to customers.

The phrase electronic agent can also have an interpretive impact tied to value as an institution that has special handling authority and authority for banks. The handling of bank electronics can provide a new culture to the bank that reflects legal values substantially. An example of a bank's handling of employees who are involved in buying and selling customer data on the black market to offer a bank product. Is this allowed for the reason of partner cooperation? Or is it part of a culture that cannot be neutralized?.

Legal culture can be interpreted as an action that is faced with the legal system, beliefs and values and expectations. Behavior that is reflected both positively and negatively that is tied to values and norms (Sofiani, Trianah, and Heris Suhendar, 2024: 61-75) The current legal culture on the handling of cyber and data security by banks towards customers reflects the effectiveness of the law on the actualization of information laws and electronic transactions. The hacking of several bank data, namely Bank Indonesia on January 21, 2022, Bank BSI May 2023 and most recently Bank BRI on December 18, 2024, which always raises questions in the community whether it has an impact on losses to customers directly or not. Direct handling by the authorities or the bank itself is felt necessary to provide comprehensive clarity.

The birth of the ITE law is the answer to the high number of electronic crimes that occur in Indonesia, allegedly electronic crimes in banks can cause widespread harm, therefore, optimal institutional mitigation is needed both civilly and criminally. (Pakpahan, Bani David Soaloon, et al, 5.2 2023) Data collection without the customer's consent should not become a culture on the grounds of partners, because the mechanism and provisions of data privacy have been regulated by Law Number 27 concerning personal data protection, Article 16 (2), whose substance is as follows:

> "destruction, and/or deletion of personal data; f. The processing of personal data is carried out by notifying the purposes and activities of the processing, as well as the failure of the protection of personal data; g. Personal data is destroyed/deleted after the retention period ends based on the request of the personal data subject, unless otherwise specified by laws and regulations; and h. The processing of personal data is carried out responsibly and can be proven." (Denisa, Adinda Putri, Muhamad Amirulloh, and Helitha Novianty Muchtar, 2023)

The clause is used in an agreement between the customer and the bank which in its implementation is not easy to implement, on the one hand the bank has insurance or finance partners and the other is categorized as a part affiliated with the bank. In the practical order, the customer does not know where the data is obtained, even though it does not have a direct impact on material losses, but the above clause is set aside because of the potential as a new consumer.

The fundamental understanding of Stufenbau theory (Stufenbau des Rechts Theorie) focuses on the individual's awareness of values, principles, and legal norms, each of which has its components and concepts (Kurniawan, Faizal, et al. 2023: 192-211.) The meaning of the word "without written consent" is a norm that cannot be interpreted otherwise, but in practice, it can be set aside as commonplace. This is the importance of a legal culture that can provide legal awareness both individually and socially. Personal data is easily transferred through various internet platforms and applications, such as names, addresses, telephone numbers, and other information collected by service providers, including banks, which are not essentially deleted when they no longer have a contractual relationship, even if this is done lawfully for marketing purposes (Priliasari, Erna. 2023: 261-279) Smart regulation is an integral part of the technological perspective that aims to regulate regulation (Zaman, Muhamad Nafi Uz. 13.1, 2024). The ITE Law has administrative nuances that regulate information traffic and electronic transactions, but contains criminal threats Essentially, the ITE Law emphasizes preventive measures rather than repressive actions, as seen in cases charged under the ITE Law regarding cybersecurity cases. So far, there has been no one prosecuted for hacking bank customer data.

The security of customer data and funds is a priority for banks, these provisions are a guarantee as the implementation of good corporate governance. Preventive efforts have been made by the bank and customers, but in their implementation there are areas where customers take actions that cause material losses such as cases of skimming, carding, gendam, fishing, vishing, fraud, fraud and other methods that cause losses.

Kasus	Terminologi	Kerugian	Tanggung jawab
Skimming/Carding	Crime of data card theft using a special device on ATM or EDC machines	Materil	Customer
Phissing	Crime by tricking customers through fake emails or messages to obtain passwords or PINs	Materil	Customer
Gaslighting	Crime with the ability to manipulate someone's consciousness	Materil	Customer
Phissing	Fraud committed by phone to obtain personal information	Materil	Customer
Fraud	Fraud committed to gain financial benefits illegally	Materil	Bank
Forgery	Creation of forged documents and signatures intended to deceive	Materil	Bank
Data Hacking	Cybercrime of customer data hacking resulting in data and customer funds leakage	Materil	Bank

Table II. Responsibilities of Banks and Customers

Source: summarized by the author from various sources

Based on the explanation presented in the table, which provides the basis for whether the responsibility is imposed on the bank or the customer, it depends on the condition of the case and the actions taken. The heavy point is the action in the form of negligence or intentionality committed by both the bank and by the customer, the common thread is the negligence committed by the customer, then the obligation to compensate for losses is the customer such as Skimming/Carding, Phissing, Gaslighting, Phissing, Fraud, Forgery, Data Hacking. It is indicated that it is negligence committed by the customer, and then the customer bears the loss. Likewise, negligence committed by banks such as hacking customer data that results in losses, the bank must compensate the customer for material losses such as in the case of wrong account transfers, fraud committed by bank employees, falsification of customer data that is not verified by the bank so as to cause customer losses and bank data overflow that directly causes material losses to customers.

The responsibility for compensation is difficult to prove whether it is negligence of the bank or the customer can be resolved through consensus deliberation or mediation. If it is not achieved, it is possible to file a lawsuit through litigation. Financial literacy in the use of mobile banking and other financial technology devices is very important to be understood by the public as a prevention of negligence in customers and to protect against the possibility of fraud to the bank.

Reactualization Strategy to Improve Cyber Security of Banking Customer Data and Funds

Several incidents of cyber attacks have been experienced by Bank Syariah Indonesia (BSI) and Bank Rakyat Indonesia (BRI). The case of service disruption experienced by Bank Syariah Indonesia (BSI) since May 8, 2023, has led to speculation about a cyber attack allegedly carried out by a hacker group (diakses 3 Juni 2025). The attack resulted in the BSI system being completely shut down for several days, so customers could not access mobile banking, ATM, or teller services at branch offices.

The case of a cyberattack involving the Bashe hacker group against Bank Rakyat Indonesia (BRI) on December 18, 2024 highlights the increasing threat of cybercrime, especially in the banking sector. According to reports, Bashe's group managed to infiltrate the BRI system and steal sensitive data, then gave an ultimatum to release the data if the ransom demand was not fulfilled within four days. As proof of authentication, they include examples of stolen data (diakses 3 Juni 2025)

Data theft is one of the cyberattacks on the banking sector and is a very crucial issue in this digital era, considering the increasing development of technology that allows access to personal data widely. Personal data, as described by Bozkurt, includes information that can directly or indirectly identify an individual, such as ethnic origin, health information, education data, residential address, banking or credit card information, to a person's ideological views and beliefs (Bozkurt, Aras. pp. 2023: 1237-1254) With the increasing activity of people in electronic media, personal data is often exposed more than the data owner wants. For example, Android-based apps often ask for access to personal data such as phone contacts, messages, and user conversation details as a condition of installing the app.

One of the preventive steps that can be taken is to strengthen regulations related to personal data protection, including the application of the principle of explicit consent from the data owner before the data can be accessed or used by third parties. This is in line with the provisions of personal data protection regulated in various laws in many countries.

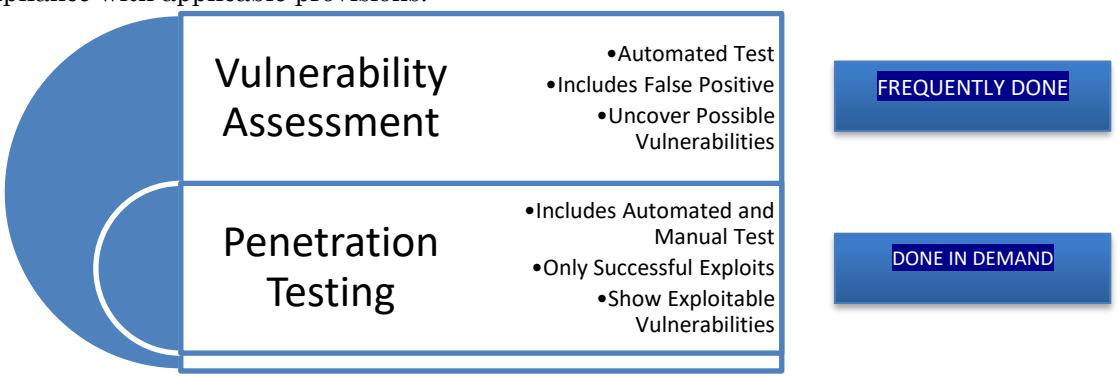
In order to increase resilience and cybersecurity in the banking sector, the Financial Services Authority (OJK) has issued Circular Letter of the Financial Services Authority Number 29/SEOJK.03/2022 concerning Cyber Resilience and Security for Commercial Banks. This circular is a follow-up to the Financial Services Authority Regulation Number 11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks (POJK PTI), which aims to provide more detailed implementation guidelines related to cyber risk management in banks. In preventive legal efforts to anticipate cyber attacks, commercial banks are required to implement strategic measures, such as Indarta explaining strengthening information security management systems, improving cyber threat early detection capabilities, and developing effective risk mitigation mechanisms (Indarta, Yose, 2025)

The Financial Services Authority (SEOJK) Circular Letter Number 29/SEOJK.03/2022 concerning Cyber Resilience and Security for Commercial Banks regulates the obligation of banks to carry out cybersecurity testing as described in Chapter VII. These tests include two main types: tests based on vulnerability analysis and tests based on scenarios. Testing based on vulnerability analysis aims to identify weak points in the bank's information technology system through a vulnerability identification process followed by periodic penetration testing. The results of this test must be reported to the OJK as part of the report on the current condition of the bank's information technology implementation.

Meanwhile, the scenario-based testing is designed to validate banks' readiness to address and recover from cyber incidents through simulated attacks that are carried out in a controlled and closely monitored manner, at least once a year. The results of this test must also be submitted to the OJK no later than 10 working days after the test is completed. The results of the cybersecurity test are submitted to the Board of Directors to serve as a basis for improving governance, policies, procedures, internal control, as well as increasing the capacity and awareness of Bank employees towards cyber resilience and security. In addition, test results must also be reported to the Financial Services Authority (OJK) with certain conditions.

For testing based on vulnerability analysis, the results must be attached to the Bank's IT Current Condition Report and submitted no later than 15 working days after the end of the reporting year. For example, the results of penetration tests conducted in March, July, and November 2022 must be compiled and reported to the OJK no later than January 20, 2023. Meanwhile, cybersecurity testing based on scenarios must be submitted no later than 10 working days after the test result report is completed, according to the format specified in Appendix VI of the OJK Circular Letter.

The report at least contains a summary of the test implementation, lessons learned, and plans or improvements that have been made. For example, if cybersecurity testing with a ransomware attack scenario is carried out on November 3, 2023 and the report is completed by November 14, 2023, then the results must be submitted to the OJK no later than November 28, 2023. Banks are given the flexibility to carry out cybersecurity testing independently or use the services of a third party, as long as they continue to observe the principles of prudence and compliance with applicable provisions.



Gambar. 1. Perbedaan Proses Pengujian Keamanan Siber

Vulnerability assessment is the process of identifying security vulnerabilities that are carried out automatically using certain scanning devices or tools to detect possible security vulnerabilities (Yu, Miao, Jianwei Zhuge, Ming Cao, Zhiwei Shi, and Lin Jiang, 2020) This process aims to provide a report on the vulnerabilities found without exploiting those vulnerabilities. Due to its automated nature, vulnerability assessments are often conducted on a regular basis, such as monthly or quarterly, to adapt to technological developments and dynamic security threats.

Meanwhile, penetration testing is a more in-depth test by utilizes vulnerabilities that have been identified to simulate attacks from external parties. This process not only relies on automated tools but also involves human elements to identify and exploit weaknesses in business logic that automated tools may not be able to detect. (Edwards, Dr Jason, 2024: pp. 371-412.) Thus, penetration testing provides a clearer picture of the extent to which an external attacker can exploit the vulnerability and the maximum business impact it can cause. Due to its complex and in-depth nature, penetration testing is typically conducted on an annual basis, on demand, or when a new system, application, or device is deployed.

The fundamental difference between these two methods lies in the approach and frequency of their implementation (Shah, Sugandh, and Babu M. Mehtre, 2015). Vulnerability assessments are more often conducted to detect vulnerabilities in general, while penetration testing aims to evaluate the real impact of these vulnerabilities on the banking system. With the combination of these two methods, banks are expected to be able to significantly increase their cyber resilience, minimize the risk of cyberattacks, and protect the interests of customers and the stability of the national financial system. Therefore, compliance with the provisions in SEOJK Number 29/SEOJK.03/2022 is a legal obligation that must be fulfilled by every commercial bank as part of their responsibility in maintaining cybersecurity.

The rapid development of digital banking technology aligns with the strict implementation of regulations on central bank digital currencies (CBDCs) based on accounts. This system enables digital currencies to be managed through ledger entries in accounts held and regulated by banks, with the central bank determining interest rates and usage rules (Bindseil, Ulrich, 2019: 303-335) Given that the current banking infrastructure is largely account-based, the implementation of an account-based retail CBDC can leverage existing technology, thus only expanding access to its use. However, it is important to ensure that the regulation of retail CBDCs does not differ significantly from the regulation of wholesale electronic fund transfers, except when it comes to consumer protection. For example, regulations such as Article 4A of the Uniform Commercial Code (UCC) in the United States can be an important reference because they cover in detail the rights, obligations, and responsibilities of banks and intermediaries in electronic fund transfers. Article 4A has also influenced international regulations, including the Model Law on International Credit Transfers from UNCITRAL and the European Directive on Payment Services (Geva, Benjamin, 2020).

With such a comprehensive legal framework, CBDC management can be carried out more securely and transparently, while minimizing the risk of cyberattacks that can harm the banking sector. One approach that can be taken is to adopt a clear and consistent legal framework, as set out in Article 4A. This article provides guidance on the transfer of funds, including the allocation of rights, liabilities, and responsibilities among financial institutions and their customers involved in wire transfer payments. In this context, the transfer of funds from one electronic bank account to another should be treated the same, whether it is a retail or wholesale transfer.

For example, a retail customer can initiate a fund transfer by sending a payment order to their bank. The bank, provided that the customer's account has sufficient funds, then sends a payment order through a system such as Fedwire to the receiving bank. The recipient's bank, after receiving the funds, will credit the beneficiary's account. Although Article 4A was originally designed for wholesale wire transfers, some of the consumer protection provisions discussed may provide an appropriate regulatory framework for retail Central Bank Digital Currency (CBDC) transactions. In this regard, it is important to consider the key legal issues of retail CBDCs: risk of loss, protection against counterfeiting, data privacy and storage, anti-money laundering, and consumer protection (Jans, Jan A. 2024: pp. 195-229).

1	*Risk of loss*	Risk of loss includes at least three risks: mistakenly transferring funds to the wrong person; fraud risk, including fraudulently transferring funds to a wrong person; and credit risk, including the risk of the 'receiving bank' paying out before being paid.
2	*Counterfeiting protection*	The replication or manufacture of a financial instrument […] with the intent to defraud an individual, entity, or government.
3	*Privacy and data keeping*	Central bank digital currencies may help to centralize data about the money supply.
4	*Anti- money-laundering laws*	AML laws generally follow the recommendations of the Financial Action Task Force (FATF), an inter- governmental body.
5	*Consumer protection*	covers many domestic and international electronic funds transfers, it was designed for use by relatively sophisticated parties, such as businesses and financial institutions.

Table. 3. Key of Central Bank Digital Currency (CBDC)

Preventive legal measures in dealing with banking cyberattacks are important steps that must be taken to protect the financial system and consumers. The risk of losing funds, such as misplaced transfers to the wrong party, fraud risk, and credit risk, requires strict oversight through regulation and technological safeguards. Protection against falsification of financial documents

must also be strengthened to prevent criminal acts that can harm individuals, institutions, or governments. In addition, privacy management and data storage are a priority, especially with the potential use of central bank digital currencies (CBDCs) that can centralize data related to the money supply. The implementation of anti-money laundering (AML) laws following the recommendations of the Financial Action Task Force (FATF) must be enforced to prevent the flow of illegal funds (Yeh, Stuart S. 2022)

Consumer protection should also be expanded, not only to include domestic and international electronic fund transfers, but also to ensure that the parties involved have an adequate understanding of their risks and responsibilities (Hendrayana, I. Gede, Degdo Suprayitno, Loso Judijanto, Ferry Kosadi, Sri Yani Kusumastuti, and Sepriano Sepriano, 2024) With these preventive measures, the banking system can be better prepared to face cyber threats and protect the interests of all parties involved. As such, the implementation of a comprehensive and consistent legal framework is essential to mitigate the risk of cyberattacks in digital banking. This not only protects financial institutions but also provides better protection for consumers in an increasingly digitally connected banking ecosystem.

One method that can be used to improve security is through authentication and identity management of online banking using out-of-band channels. These channels include other devices and methods that are not connected to the Internet, thus providing an authentication path that is beyond the reach of the cyber attacker (de Melo, Laerte Peotta, Dino Macedo Amaral, Robson de Oliveira Albuquerque, Rafael Timóteo de Sousa Júnior, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba, 2024) The basic concept is that cyberattacks cannot be coordinated on two physically separate channels. SMS- based schemes that provide strong authentication can improve the overall usability and security of the scheme (Fitria, Kaira Milani, 2023)

There are two types of authentication associated with online banking services: user authentication and data origin authentication. In user authentication, the main objective is to ensure that the identity of the entity, whether human or not, is as claimed and feasible to access the banking system (Hammood, Waleed A., Ruzaini Abdullah, Omar A. Hammood, Salwana Mohamad Asmara, Mohammed A. Al-Sharafi, and Ali Muttaleb Hasan, 2020) Meanwhile, data origin authentication ensures that the data comes from the expected source and does not undergo changes during transit. Therefore, user authentication establishes the feasibility of communication between the user's device and the bank, but it does not guarantee that each data packet is the intention of that user and not the result of malware activity. Data origin authentication aims to address this threat by authenticating each transaction itself.

A commonly used method is the use of One-Time-Passwords (OTPs), which are based on sending an authorization code to the user's phone to authenticate financial transactions (Yi, Poh Xin, Intan Farahana Kasmin, Salmiah Amin, and Nur Khairunnisha Zainal, 2022) The user then manually enters the code into the user's terminal to confirm the correctness and complete the transaction. The use of user authentication and/or transaction authentication alone is considered insufficient to prevent malicious software attacks, man-in-the-middle attacks, or a combination of both, which can manipulate transaction data sent through the user's computer or displayed in a web browser, known as man-in-the-browser attacks (Mallik, Avijit. 2019) To improve the effectiveness of out-of-band devices, the researchers proposed two implementations that consider convenience, mobility, integration, administration, and cost, with better whitelist management.

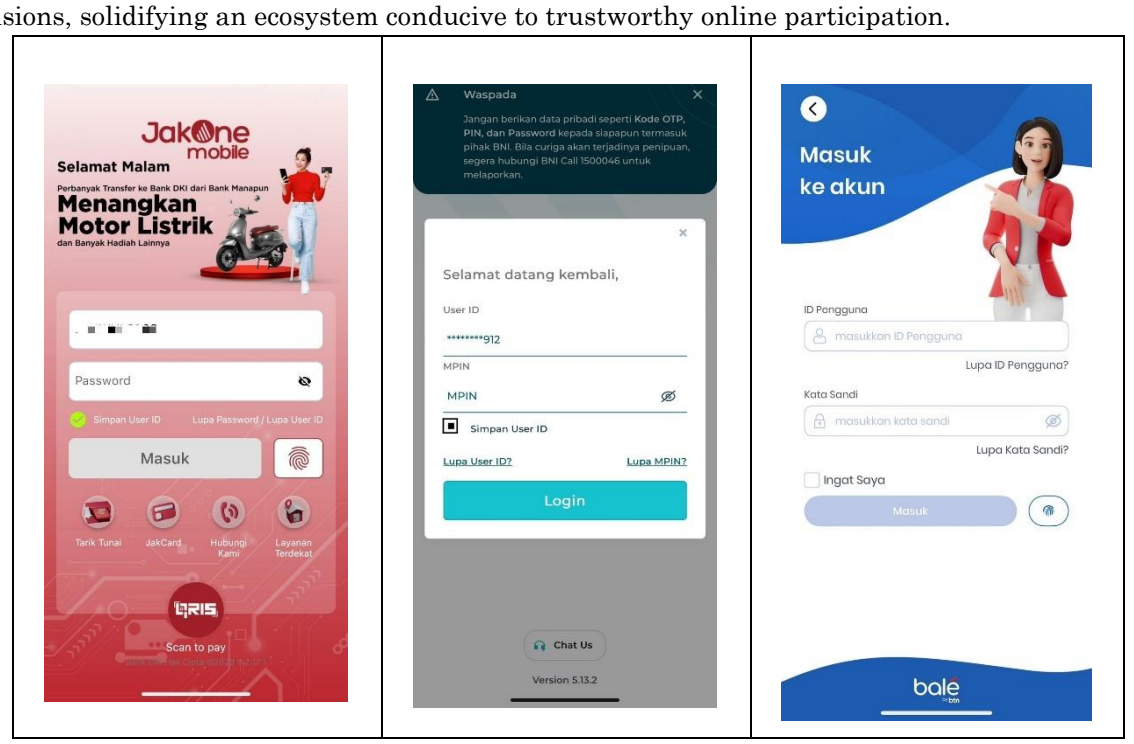
Attacks on online banking services can be classified into two main categories, namely social and physical or software-based attacks. In social attacks, perpetrators attempt to convince users to take certain actions, such as revealing user IDs and passwords or approving fraudulent transactions. The main defense against this type of attack is user education and vigilance (Najib, Warsun, and Selo Sulistyo, 2020) Therefore, one of the main goals is to create a technical environment that allows users to exercise vigilance more effectively. On the other hand, a physical attack involves attempting to steal a user's token, hack a chip card, or circulate a fake device.

Although these types of attacks are not aimed at many people and are relatively easy to investigate with standard methods, the biggest threats come from software-based attacks.

Software attacks are becoming the most common threat for several reasons. First, these attacks can be carried out remotely by spreading malware through infected emails or websites (Roseline, S. Abijah, and S. Geetha, 2021) Second, it is easier to launch these attacks because the necessary knowledge and tools are widely available on the internet at a low cost. Third, software attacks are difficult to track because the perpetrators often use botnets and hosting servers that are located in other countries with different jurisdictions. Therefore, optimizing cybersecurity in banking requires a holistic approach that includes cutting-edge technology, user education, and a stronger international legal framework to address cross-border threats.

To access the system, users are required to log in using their user ID and password, accompanied by a CAPTCHA for additional security. For the execution of transactions, it is mandatory to utilize either a token or a One-Time Password (OTP), which will be sent directly to the registered mobile number of the customer. These measures are implemented to ensure the integrity and confidentiality of the system, adhering to established legal and regulatory standards for secure digital interactions.

These robust security policies are carefully but rigorously established to protect both the platform's operational integrity and the sensitive personal data of users. Implementing these controls not only acts as a strong barrier against potential risks but also ensures lawfully secure digital trade and information exchange. Compliance with prevailing industry-specific regulations further reinforces the reliability designed to instill confidence among users. By meticulously attending to security nuances, these practices jointly endeavor to create a safe environment free from intrusions, solidifying an ecosystem conducive to trustworthy online participation.



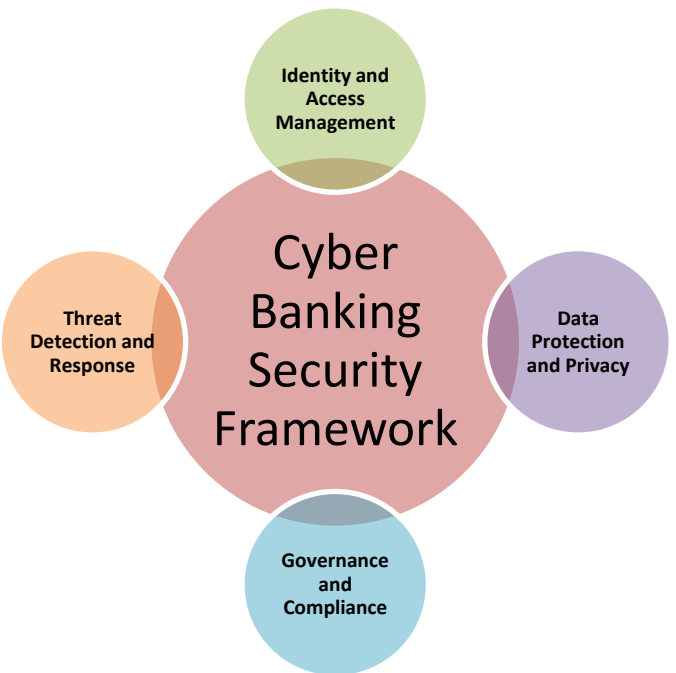
Picture. 2. Login Screen

Users are greeted with a home screen, which provides three main options. The main focus lies on the "Log On" option, which redirects the user to the authentication screen. This stage is critical because it is the entrance to sensitive banking information. After selecting the "Log On" option, the user is redirected to the authentication screen, where the identity verification process is performed. Security at this stage must be optimized through the application of the latest encryption technology, multi-factor authentication, and real-time monitoring of data traffic to prevent potential cyberattacks.

One of the options on the JAKONE Bank DKI screen is the "Scan to Pay" feature, which is a digital payment method that allows users to make transactions by scanning a QR code using their device. In a legal context, the use of this feature must comply with applicable regulations related to electronic transactions, personal data protection, and cybersecurity. Users are expected to ensure that the scanned QR code is from a trusted source to avoid potential fraud or data misuse. In addition, payment service providers are required to meet security standards set by relevant authorities to protect users' financial information. Thus, the implementation of this feature is expected to support transaction efficiency while providing adequate legal protection for all parties involved.

Meanwhile, BNI Mobil Bank BNI displays a warning to users not to provide personal data such as OTP Codes, PINs, and Passwords to any party, including Bank BNI. This is an effort to optimize the cyber security of banking customer data. This warning is important because fraud is common where irresponsible parties try to obtain sensitive customer information to be used illegally. Therefore, this application urges users to immediately contact the BNI call center if they suspect fraudulent attempts. In addition, this application also asks users to log in using User ID and MPIN (Mobile Personal Identification Number) as a form of authentication and identity verification. This is an important step in keeping users' accounts secure and protecting their personal data.

The cybersecurity framework in optimizing the protection of banking customer data includes controlling operational conditions, the first threat entry point, and known deployment strategies. Network entry points are identified through the separation between the external physical space and the banking cyber physical area, where firewalls and routers are installed on the network access points. Network policy and firewall managers are responsible for defining and configuring deployment strategies and procedures.



Picture. 3. Cyber Banking Security Framework

One of the important components is Identity and Access Management which ensures that only authorized users can access the banking system and perform legitimate actions, through user authentication, authorization, and access control (Indu, I., PM Rubesh Anand, and Vidhyacharan

Bhaskar, 2018) In addition, data protection and privacy are top priorities by implementing data encryption, access control, and data backup and recovery mechanisms to maintain the confidentiality, integrity, and availability of customer information. Detection and response to cyber threats must also be optimized through security monitoring, incident response, and the use of threat intelligence to counter attacks such as malware, phishing, and unauthorized access attempts. Finally, governance and compliance with regulations must be ensured through the implementation of security policies, risk management, and compliance with applicable standards and regulations in the banking industry.

Threat optimization and validation are associated with application security, which can be achieved through the application of the "least privilege" principle to meet operational requirements. Vulnerability checks on applications can also help with the optimization and validation process. Controlling operational conditions includes the purchase of secure software and hardware, security settings for software and hardware on workstations, laptops, and servers, and ongoing vulnerability evaluation and remediation. Cybersecurity defense strategies, mobile and wireless device management, data recovery capability plans, and security skills evaluation and training are part of the control to prevent initial attacks. In addition, the rules for known deployment strategies involve the configuration of network devices such as firewalls, switches, and routers.

Access control to network ports, services, protocols, administrative rights management, border defense implementation, security audit log maintenance, account monitoring and analysis, security incident response, and data recovery capabilities are all important steps in optimizing and validating risks to protect banking customer data as a whole. In addition, periodic audits of the application security system must be carried out to ensure that customer data protection is maintained from evolving threats. The implementation of these measures will support the protection of customer privacy and trust in banking institutions.

CONCLUSIONS

The actual condition of cybersecurity to protect funds and data is still partial and not comprehensive, this is indicated by the weak system to mitigate the security of customer data and their fund deposits. These indications can be verified from the following: first, there are no repressive actions against cyber hackers who are prosecuted due to weak verification of evidence and regulations in the law enforcement process, for example the sale of customer data online, second, the accessibility of law enforcement to limit the jurisdiction of cyber crime perpetrators who are out of reach, third, the expensive process of proving cyber law with adequate instruments. Strategies that can be carried out by strengthening cyber law enforcement instruments, reformulating provisions in laws and regulations that lead to efficient and effective preventive and repressive actions.

BIBLIOGRAPHY

A. Books

Muhammad, A. (2004). Hukum dan Penelitian Hukum, Bandung, Citra Aditya Bakti.

Indarta, Y. (2025). *Cyber Law: Dimensi Hukum dalam Era Digital*. Pustaka Galeri Mandiri.

Hendrayana, I. G., Suprayitno, D., Judijanto, L., Kosadi, F., Kusumastuti, S. Y., & Sepriano, S. (2024). *E-Money: Panduan Lengkap Penggunaan dan Manfaat E-Money dalam Era Digital*. PT. Sonpedia Publishing Indonesia.

B. Papers/Articles/Proceedings/Research Results

Anand, G., Nugraha, X., & Putri, D. E. K. (2023). Formulasi penegakan hukum yang sistematis terhadap penyelesaian sengketa konsumen e-commerce terkait tidak dipenuhinya janji

oleh pelaku usaha: Sebuah upaya mewujudkan perfect procedural justice. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

Arbani, T. S., & Putri, A. H. (2024). Legal Evaluation Strategy to Bridging the Regulatory Gap in Facing Technological Developments and Globalization in Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *13*(3).

Aris, M. S., & Putri, D. E. K. (2024). Legal Audit sebagai Mekanisme Penyelesaian Disharmonisasi Peraturan Perundang-Undangan. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *13*(1).

Ayyas, M., Fauzi, A., & Widodo, S. (2024). Studi Komparatif Teknik Analisis Keamanan Sistem Informasi e-Government: Penetration Testing VS Vulnerability Assessment. *SATIN-Sains dan Teknologi Informasi*, *10*(1), 36-44.

Bindseil, U. (2019). Central bank digital currency: Financial system implications and control. *International Journal of Political Economy*, *48*(4), 303-335.

Prahassacitta, V. (2023). SARANA PENAL DAN NON-PENAL DALAM MELINDUNGI KONSUMEN E-COMMERCE. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

de Melo, L. P., Macedo Amaral, D., de Oliveira Albuquerque, R., de Sousa Júnior, R. T., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). A Secure Approach Out-of-Band for e-Bank with Visual Two-Factor Authorization Protocol. *Cryptography*, *8*(4), 51.

Denisa, A. P., Amirulloh, M., & Muchtar, H. N. (2023). Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

Destyarini, N. (2024). Ensuring Personal Data Protection in Telemedicine Services. *Jurnal Dinamika Hukum*, *24*(2), 218-233.

Durianto, D., Hasana, D., Fareha, N., & Maharani, D. N. (2025). The Challenges of Sharia Fintech Regulation in Indonesia: A Global Comparative Analysis. *Jurnal Hukum*, *41*(1), 19-30.

Edwards, D. J. (2024). Vulnerability assessment and penetration testing. In *Mastering cybersecurity: Strategies, technologies, and best practices* (pp. 371-412). Berkeley, CA: Apress.

Fadia, Y., & Nusantara, M. A. Z. (2023). Strengthening Anti-Money Laundering Framework in Online Banking: Bank Indonesia's Initiatives and Countermeasures. *Jurnal Hukum*, *39*(2), 252-269.

Fitria, K. M. (2023). Analisis serangan malware dalam perbankan dan perencanaan solusi keamanan. *Jurnal Informatika dan Teknik Elektro Terapan*, *11*(3).

Geva, B. (2020). Electronic Payments: Guide on Legal and Regulatory Reforms and Best Practices for Developing Countries. *International Trade Centre*.

Hammood, W. A., Abdullah, R., Hammood, O. A., Asmara, S. M., Al-Sharafi, M. A., & Hasan, A. M. (2020, February). A review of user authentication model for online banking system based on mobile IMEI number. In *IOP Conference Series: Materials Science and Engineering* (Vol. 769, No. 1, p. 012061). IOP Publishing.

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, *21*(4), 574-588.

Istiyowati, L. S. (2018). Fitur-Fitur Layanan Internet Banking Pada Bank Di Indonesia. *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *6*(3), 1589-1600.

Jans, J. A. (2024). Anti-Money Laundering and the Allocation of Responsibilities Between Banks and Non-Banks. In *Electronic Payments in the European Market: Creating a Level Playing Field between Banks and Non-Banks* (pp. 195-229). Cham: Springer Nature Switzerland.

Kurniawan, F., Thalib, P., Subhan, M. H., Jansen, B., & Abd Ghadas, Z. A. B. (2023). Justice as a Meta Value of Corrective Justice in Providing Restitution for Unjust Enrichment: A Study on Rules, Norms, Principles, and Foundation. *Jurnal Hukum*, *39*(2), 192-211.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *International journal of data and network science*.

Mentari, N., Nugraheni, N., & Annas, M. (2023). Legal Protection of HARA Platform Users on the Service of Electronic Data Interchange. *Jurnal Hukum Novelty (1412-6834)*, *14*(1).

Najib, W., & Sulistyo, S. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, *9*(4), 375-384.

Nofrial, R., Abood, T. A., Shihab, H. A., & Susilo, A. B. The Consumer Protection in The Balance of Business Actors and Consumers: A Paradigm of Justice. *Jurnal Hukum*, *41*(1), 73-91.

Omokanye, A. O., Ajayi, A. M., Olowu, O., Adeleye, A. O., Chianumba, E. C., & Omole, O. M. (2024). AI-powered financial crime prevention with cybersecurity, IT, and data science in modern banking. *International Journal of Science and Research Archive*, *13*(3).

Pakpahan, B. D. S., Parameshwara, P., Pakpahan, K., Saota, M. C. N., & Tambunan, F. O. (2023). Tinjauan Yuridis Kejahatan Di Dalam Sistem Elektronik Pada Rekening Virtual. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, *5*(2), 1691-1708.

Pratiwi, A. (2022). Evaluation of Automated Configuration Management Tools in Achieving Least-Privilege Access Policies for E-Retail. *International Journal of Applied Business Intelligence*, *2*(12), 23-30.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

Putra, G. A., Taniady, V., & Halmadiningrat, I. M. (2023). Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunanya. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).

Putranti, I. R. (2022). Principle of Technological Neutrality in Trade Facilitations: A Legal Perspective. *Jurnal Hukum Novelty (1412-6834)*, *13*(2).

Roseline, S. A., & Geetha, S. (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers & Electrical Engineering*, *92*, 107143.

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27-49.

Sofiani, T., & Suhendar, H. (2024). The Settlement Model of Non-Performing Financing Which is More Effective and Legal Justice in Sharia Financing Companies. *Jurnal Hukum*, *40*(1), 61-75.

Yeh, S. S. (2022). New financial action task force recommendations to fight corruption and money laundering. *Laws*, *11*(1), 8.

Yi, P. X., Kasmin, I. F., Amin, S., & Zainal, N. K. (2022). Implementation of One-Time Password in Online Banking System Among Malaysian Bank Users to Reduce Cyber Fraud. *International Journal of Data Science and Advanced Analytics*, *4*, 20-26.

Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. *Future Internet*, *12*(2), 27.

Zaman, M. N. U. (2024). Smart Regulation As A New Approach In Regulatory Reform In Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *13*(1).

C. Internet

https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang (diakses tanggal 08 Mei 2025)

https://kabarbursa.com/market-hari-ini/107365/diduga-terjadi-kebocoran-data-begini-penjelasan-bri (diakses tangggal 09 Mei 2025)

https://lpem.org/special-report-vol-1-no-1-may-2023-isu-keamanan-siber-perbankan-dan-potensi-bank-run/ (diakses tanggal 08 Mei 2025)
https://www.bbc.com/indonesia/articles/cn01gdr7eero (diakses 3 Juni 2025)
https://www.google.com/search?sca_esv=68ea10725fc9b20e&q=Data+Statistik+pengguna+Mobile+Banking+di+Indonesia+2024&sa=X&ved=2ahUKEwi-kPeGpJWNAxVQ4jgGHWgrBqkQ1QJ6BAg-EAE&biw=1366&bih=589&dpr=1 (diakses tanggal 09 Mei 2025)
https://www.tempo.co/ekonomi/bca-catat-4-miliar-serangan-siber-ke-sistem-perbankan-pada-2024-1210740 (diakses tanggal 09 Mei 2025)
https://www.tempo.co/sains/daftar-serangan-ransomware-ke-lembaga-keuangan-indonesia-bi-bsi-dan-terbaru-bri-1183490 (diakses 23 April 2025)

https://www.tempo.co/sains/mengenal-bashe-kelompok-ransomware-yang-diduga-serang-bank-bri-1183441 (diakses 3 Juni 2025)

D. Regulation

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
Undang-Undang Nomor Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen
Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektornik sebagaimana diubah dengan Undang-Undang Nomo 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
POJK Nomor 21 Tahun 2003 Tentang Layanan Digital Oleh Bank Umum
SEOJK Nomor 29/SEOJK.03/2022 Tentang Ketahanan dan Keamanan Siber bagi Bank Umum