JOURNAL OF LEGAL AND SOCIAL CHANGES
Scientia Plus Corp
P-ISSN: 00000
E-ISSN: 00000

Legal Protection for Customers in Digital Banking Transactions: A Case Study of Bank Syariah Indonesia (BSI)

Angga Praditya Suhendar[1*]

[1] Faculty of Law and Political Science, Muhammadiyah University of Surakarta, Sukoharjo, Center Java, Indonesia, 57169
[*] C100210199@student.ums.ac.id

Article

Keywords:
Industrial Digitization; Digital Banking; Personal Data Protection; Effectiveness; Phishing

Article History
Received: Apr 14, 2026;
Reviewed: Apr 27, 2026;
Accepted: Apr 28, 2026;
Published: May 01, 2026;

Abstract

The objective of this study is to investigate the transition to industrial digitalization, with a specific focus on the transition of bank security to digital banking. However, this growth is also accompanied by risks arising from a lack of personal data protection, which can negatively impact the development of digital banking services. This includes phishing attempts. This is a method used to steal user information with the aim of obtaining user IDs and passwords. Therefore, a qualitative legal approach is used in this study. Data sources for this study include primary and secondary data. The research findings indicate that, according to Lawrence M. Friedman's theory, a legal system consists of three main components: legal structure, legal substance, and legal culture. These three elements interact with one another to shape the effectiveness of the legal system. Theoretically, legal restrictions on phishing in Indonesia have not yet been fully effective. This is evident from existing regulatory and law enforcement factors; while they play a crucial role in the administration of justice, they have not yet been able to reduce the number of phishing cases in Indonesia.

INTRODUCTION

The increasing digitalization of industry means that many existing activities will also follow this trend. Society has now transitioned from the era of industrialization to the era of religious reform. This phenomenon has led to numerous paradigm shifts across all global sectors. Technological innovation not only helps improve the quality of life but also contributes to the transformation of the financial sector, which is currently undergoing significant changes in the banking industry(Sugihyanto & Jansen Arsjah, 2023). The principle of prudence serves as the foundation of banking in Indonesia. According to Law No. 10 of 1998 of the Republic of Indonesia, a bank is a

business entity that collects funds from the public and channels these resources back to the public in the form of loans or through various financial mechanisms, with the aim of improving their welfare and standard of living(Sugihyanto & Jansen Arsjah, 2023).

Indonesia, as a developing country, is characterized by various development programs implemented across various sectors of national life, particularly in the field of internet media. All forms of existing activities are increasingly being shifted to the digital realm. This is evident from the growing use of communication tools and technologies such as computers, laptops, mobile phones, and the internet among the public. Technological advancements contribute positively by facilitating communication and simplifying complex tasks. Advances in digital banking have transformed how individuals interact with financial institutions, offering more choices and convenience in managing their personal finances. This leverages digital technology to meet customer needs in response to the rapid evolution of the digital economy(Suharbi & Margono, 2022).

Many banks operating in Indonesia have, over time, also leveraged technology to innovate and become advanced banks by developing their own proprietary mobile apps, such as Livin by Mandiri, BSI Mobile, Octo Mobile by CIMB Niaga, BRI Mobile, BNI Mobile, and many others. The advancement of the internet, particularly as a medium for widespread information dissemination, carries serious implications regarding misuse, where certain parties may exploit the internet to gain illicit benefits by stealing personal data including user IDs or passwords which severely harms users of mobile banking or digital banking services. Cases of fraud or fraudulent acts in 2022 and 2023 are recorded in police data on the PUSIKNAS (National Criminal Information Center) website; the number of fraud cases in 2022 totaled 33,167 and in 2023 totaled 35,425, with a combined total of 68,592. According to a 2022 report, the Cybercrime Directorate of the National Police's Criminal Investigation Agency recorded 5,579 incidents. The number of phishing attacks increased by approximately 41.52 percent compared to the previous quarter, which saw 3,942 attacks(Gana et al., 2024). Among various banking products and financial institutions, e-wallets and bank accounts are considered the most vulnerable to potential data breaches. In the banking sector today, there has been an increase in phishing cases using methods that deceive customers, making it appear as though the message is an official one from the bank.

On May 16, 2023, Bank BSI experienced a data breach involving 15 million pieces of personal data belonging to customers and employees, according to BBC News Indonesia. BSI is suspected to have been targeted by the attack due to the bank's weak security systems. The data includes names, phone numbers, addresses, document information, account balances, card numbers, transaction records, and much more. 3 This raises concerns that Bank BSI customers' personal data has been leaked and used unlawfully, causing harm to customers. 4 Protecting customers' personal data is of utmost importance and must adhere to banking confidentiality principles. To access electronic transaction services, customers are required to provide their personal information. This information constitutes a personal right, particularly the right to

privacy, which requires robust protection. Details such as the customer's name, date of birth, mother's name, residential address, email address, and mobile phone number must be treated with the utmost confidentiality.

It is crucial that this personal data remains free from unauthorized access, as outlined in the Electronic Information and Transactions Law No. 1 of 2023, Article 26, paragraph (1). This law stipulates that, unless otherwise provided by applicable laws and regulations, the use of any personal data via electronic media must be done with the explicit consent of the individual concerned.5 Unfortunately, there have been several cases where this personal data has not been adequately protected by existing banking security systems. The data leaked from Bank BSI on May 16, 2023, included not only customer data but also employee data, financial documents, legal documents, NDAs, and others(Ida Ayu Putu Megawati & Ni Nengah Rupadi Kertiriasih, 2024).

Bank Syariah Indonesia (BSI) must be proactive in risk management; this requires robust banking controls aimed at minimizing the likelihood of banking risks so that errors and fraud can be quickly detected and rectified, and it is highly beneficial for management in safeguarding the assets of the Islamic bank and optimizing the bank's risk management. Therefore, it is crucial to focus on risk management. Despite all difficulties and chaos, all parties must be able to participate in the development of the future of Islamic banking. The ability to manage risk is a crucial component of good corporate governance, as not all risks can typically be avoided. The strength of risk management in the financial sector lies in determining strategic steps to enhance financial security, through implementation procedures that are consistently communicated and aligned with management policies. This demonstrates that the existence of Islamic banks and the risks that may accompany them are two inseparable elements(Hani Harlan, 2025). If Islamic banks lacked the courage to take risks, they would not exist. Thus, banks exist and can survive because of their willingness to take risks; however, if those risks are not managed properly, Islamic banks may face business failure, or even bankruptcy.

There are several regulations governing this matter, including the Personal Data Protection Act No. 27 of 2022, the Information and Electronic Transactions Act No. 1 of 2023, and Article 362 of the Criminal Code regarding theft. The Personal Data Protection Act No. 27 of 2022 states "that the protection of personal data is a fundamental human right that forms part of the protection of personal autonomy; therefore, a legal framework must be established to ensure the security of personal data, in accordance with the 1945 Constitution of the Republic of Indonesia"[8], as for the sanctions imposed, they consist of administrative sanctions such as a written warning, temporary suspension of personal data processing activities, deletion or destruction of personal data; and/or an administrative fine(Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022a). The ITE Law No. 1 of 2024 states "that to maintain a clean, healthy, ethical, productive, and just digital space in Indonesia, it is necessary to regulate the use of Information Technology and Electronic Transactions to provide legal certainty, justice, and protect the public interest from all types of disturbances resulting from the misuse of Electronic

Information, Electronic Documents, Information Technology, and/or Electronic Transactions that disrupt public order," The penalties prescribed are set forth in several articles, namely Article 45A: "Any person who intentionally disseminates Electronic Information and/or Electronic Documents known to contain false information that causes public unrest as referred to in Article 28(3) shall be punished by imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah).", Article 45B "Any person who intentionally and without authorization sends Electronic Information and/or Electronic Documents directly to a victim containing threats of violence and/or intimidation as referred to in Article 29 shall be punished with imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp750,000,000.00 (seven hundred fifty million rupiah)." Article 362 of the Criminal Code on Theft states that "Any person who takes any property, whether wholly or in part belonging to another, with the intent to unlawfully possess it, shall be punished for theft with imprisonment for a maximum of five years or a fine of up to nine hundred rupiah."(Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2024) Therefore, these regulations will be highly effective, and the perpetrator may face cumulative charges for the offenses committed. Based on the elements of the acts of theft and the breach of BSI Digital Banking customer data, the perpetrator will face appropriate deterrent consequences under the aforementioned regulations.

METHOD

A research method is a scientific approach to collecting data in a systematic, logical, and structured manner to achieve specific objectives. This study employs a normative legal approach through library research, which involves examining relevant theories, concepts, and legal regulations. The research design used is descriptive, aiming to clearly depict a current event or phenomenon. The data sources used consist of secondary data, including primary legal materials such as the 1945 Constitution, Law No. 27 of 2022 on Personal Data Protection, Law No. 1 of 2023 amending Law No. 11 of 2008 on Information and Electronic Transactions, and Article 362 of the Criminal Code, as well as secondary legal materials such as books, journals, and the opinions of legal experts. Data collection was conducted through a literature review by examining various regulations, documents, books, and relevant sources, while the data analysis method used was qualitative, with data presented systematically and descriptively to facilitate understanding of the issues under study.

RESULTS AND DISCUSSION

1. Legal Regulations Regarding Phishing Attacks That Pose a Threat of Personal Data Theft from Customer Accounts in Digital Banking

The word "bank" is a familiar term in Indonesian society because the country's economy is, to a large extent, supported by the growing and evolving banking system. The transition to digital banking, as technology has permeated financial infrastructure, brings significant benefits in terms of time savings. Procedures have become simpler and more user-friendly, eliminating the need to visit physical branch offices. Customers can open an account in less than 10 minutes through an app interface that offers quick and straightforward navigation. Access is available from various locations and at any time, providing maximum convenience for customers, as well as 24/7 banking services. There are various incentives such as cashback, points redeemable for discount vouchers, and more favorable interest rate offers(Sasea & Sakmaf, 2023).

However, according to OJK records, there are several obstacles that may be encountered in the future digital transformation of the banking sector, namely challenges in the use of artificial intelligence (AI) in the banking sector, which involve several risks. Artificial intelligence has been applied in various aspects of banking, such as the automation of tasks like fraud detection, identification of money laundering transactions, or credit card application decision-making, which can carry risks in the context of artificial intelligence, including algorithmic bias. The protection of personal data and the risk of customer information loss are critical aspects. According to the OJK, the protection of customers' personal data has a significant impact on the future development of digital banking services(Akbar, 2023).

Bank Syariah Indonesia experienced a massive data breach in 2022–2023, resulting in losses for both customers and bank employees; the breach involved up to 16 million records. The breach was carried out by an anonymous website that successfully hacked BSI's website and mobile banking app, leading to significant misuse of customer and employee data. Since then, BSI has begun updating its security measures by no longer carelessly inputting customer data through public websites and no longer using WhatsApp or Telegram as communication tools for transferring customer data. Instead, BSI created a special website the name of which is not disclosed (for security reasons) to transfer customer data between branches and the central office. Data protection is a key factor in building trust in online transactions and plays a vital role in the digital transaction environment(Yuspin et al., 2023).

The risks arising from weak personal data protection can have a negative impact on the development of digital banking services. One of the main reasons is the lack of an adequate legal framework governing personal data protection, which means that local companies are not yet fully compliant with data protection standards. Moreover, low levels of financial literacy also pose a challenge. According to the OJK, a lack of understanding of digital financial literacy among bank customers can fuel cybercrime, as evidenced by data from the Cybercrime Directorate of the National Police's Criminal Investigation Agency, which shows that from January to September 2020,

there were 2,259 reports from the public regarding digital crimes. These reports include hacking of electronic systems, online fraud, data or identity theft, and data manipulation(Sriono et al., 2024).

Online fraud accounted for the highest number of complaints, indicating a lack of public understanding regarding the risks involved in digital transactions. Cybercrime also poses a significant risk. Data from the National Cyber Security Operations Center (BSSN) shows a significant increase in the number of cyberattacks, with 495 million cyberattacks in 2020 a fivefold increase compared to the previous year (228 million cyberattacks). Therefore, it is crucial for digital banking to have robust cybersecurity. Protection for customers as consumers of banking services is based on a number of consumer rights that must be safeguarded to prevent them from suffering losses caused by third parties. The following regulations govern the protection of customers as consumers(Astutik et al., 2025):

According to Article 1, Point 28 of Law No. 7 of 1992 on Banking, as amended by Law No. 10 of 1998 on Banking, it is explained that bank secrecy encompasses all information related to customers and their deposits. The bank's obligation to keep customer information confidential is explicitly regulated in Article 40(1) of Law No. 10 of 1998, and this confidentiality is limited to depositors and their deposits, except in the cases referred to in Articles 41 through 44.

Law No. 8 of 1999 on Consumer Protection applies to bank customers in general. Pursuant to Article 1(1) of Law No. 8 of 1999, the purpose is to provide all necessary measures to ensure legal certainty and to provide legal protection to consumers. Article 19(1) states that business entities, in this case the bank, are responsible for providing compensation for losses incurred by consumers as a result of using the services provided(Undang-Undang (UU) Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, 1999). Thus, regarding the issue of legal protection against customer losses resulting from system errors, the bank is obligated to provide compensation if such errors cause losses, such as a decrease or increase in the account balance, in accordance with the aforementioned legislation. However, if the customer does not suffer a loss, the bank is not obligated to provide compensation.

Law No. 27 of 2022 Law No. 27 of 2022 on Personal Data Protection (PDP Law) is a legal instrument that protects the personal data of the Indonesian public from misuse, including phishing practices. Provisions regarding personal data protection are mandated in Article 28G of the 1945 Constitution of the Republic of Indonesia, which affirms the right to protection of personal data, family, honor, dignity, and property under one's control. Furthermore, the definition of personal data is also stipulated in Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection in Article 1, paragraph 1, which explains that personal data refers to data regarding an

individual who can be identified or recognized either on their own or when combined with other information, whether through electronic or non-electronic systems(Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022b).

To date, Indonesia has not yet established a specialized agency responsible for addressing personal data issues in digital transactions, nor has the Personal Data Protection Commission (PDP) been formed. The PDP Supervisory Commission is mandated by Law No. 27 of 2022 on Personal Data Protection (PDP), which was enacted by the government and the House of Representatives in 2022. Its purpose is to ensure the well-being of Indonesian citizens(Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022c). The establishment of a Personal Data Protection (PDP) agency or commission is urgently needed to accelerate the handling of hacking cases in the country, which are becoming increasingly prevalent.

October 17, 2024, is the deadline for the full implementation of the PDP Law. This is because the government has a two-year timeframe following the law's enactment to develop implementing regulations before its enforcement. The agency or authority required to manage personal data protection in accordance with the provisions of Articles 58 through 60 of the PDP Law has not yet been established. This supervisory agency or PDP Commission is planned to be under the control of the president and will be held accountable.

Nevertheless, the PDP Act can be effectively implemented before October 2024 if the implementing regulations and the PDP Commission have been established. Therefore, it is recommended that the government immediately establish the PDP Commission in accordance with the provisions of the PDP Act. With the establishment of this institution or authority, the process of law enforcement and the imposition of sanctions can be implemented immediately.

This institution can provide technical guidance on the processing of personal data, including data collection processes for marketing purposes, compliance requirements, and highly technical regulations such as the use of cookie technology. Additionally, this commission aims to ensure the effective implementation of privacy policies and regulations related to personal data protection, given that Law No. 27 of 2022 applies to individuals, private companies, and public institutions. Therefore, the idea of establishing a personal data protection supervisory body is highly relevant.

In principle, the Personal Data Protection Supervisory Commission serves as a regulator to ensure oversight of compliance by parties that control and process personal data, resolve disputes related to personal data, coordinate and negotiate with

relevant institutions, and enforce justice if public or private entities violate applicable provisions. If the Personal Data Protection Supervisory Commission has not yet been established, some provisions of the Personal Data Protection Law may not be enforceable. This raises concerns that without a supervisory body, data leaks, hacking, and personal data breaches may not be subject to sanctions.

With the establishment of the Personal Data Protection Commission, sanctions both legal and administrative can be imposed promptly, thereby serving as a deterrent to other institutions and encouraging them to improve their protection of the personal data under their care. Through the enforcement of administrative and legal sanctions as stipulated in the Personal Data Protection Act, parties involved in the management of personal data will become more cautious regarding the security of such information. This is expected to result in effective handling of personal data security breach cases and provide better protection(Candra et al., 2024).

The Personal Data Protection Commission will have limited authority, primarily focused on handling cases related to data privacy outside the judicial system. This means that once a case enters the legal domain, the Data Protection Commission lacks the authority to participate in that process. Privacy protection is an integral part of personal data protection mandated directly by the Constitution of the Republic of Indonesia, which enshrines respect for human rights values and the equality of individual rights; thus, legislation is required(Putri et al., 2025).

This regulation is based on human rights principles and values of equality, as well as respect for individual rights, with the aim of ensuring that the privacy and personal data of the public including those who are customers or borrowers are protected and that they feel secure. One of the causes of personal information theft is phishing attacks. Phishing attacks can be carried out relatively easily and at low cost. Criminals can quickly send thousands or even millions of emails or text messages in an attempt to deceive people. Phishing is a criminal act that uses both social engineering techniques and technical methods to steal a person's personal identity data and financial account information(Bernanda Gunawan, 2024).

Phishing is not a recent phenomenon; cases of phishing have existed since 1996. This study examines legal regulations regarding phishing attacks that threaten the theft of personal data, particularly in the banking sector such as the theft of customer accounts in digital banking which occurs, for instance, by creating fake accounts and sending a website impersonating the name of a bank in Indonesia, then seemingly offering online loans or administrative fee discounts to customers. Phishing is a type of cybercrime(Sudarwanto & Kharisma, 2022).

Legal provisions regarding phishing as a form of cybercrime in Indonesia may be subject to penalties under Article 378 of the Criminal Code (KUHP), which addresses acts of fraud, as phishing is generally considered a form of fraud. Fraud as defined in Article 378 of the Criminal Code can be formulated as follows: a person who, with the intent to obtain personal gain or the gain of another in violation of the law, uses a false name or fabricates a title, through deceit or a series of lies, induces another person to hand over goods or something of value in the future, or to grant a loan or discharge a debt, is punishable for fraud by imprisonment for a maximum of four years."

The application of Article 378 of the Criminal Code in the prosecution of cybercrime cases is carried out with a specific interpretation, given the differences between the nature of cybercrimes and existing conventional crimes. Although the methods of phishing and fraud under the Criminal Code share similar elements of conduct, there are significant differences ranging from the type of criminal offense, the determination of the location where the crime occurred (*locus delicti*), to the time when the crime occurred (*tempus delicti*).

The phishing method itself, as carried out by the perpetrators, first involves sending fake messages via email, text messages (SMS), or websites to targeted potential victims, containing requests for personal information such as user IDs, PINs, or credit card numbers. Additionally, phishing criminals set a time limit for victims to provide the requested information. They also threaten with adverse consequences if the data is not provided immediately. In such situations, victims who do not take the time to think carefully are likely to provide personal information to the scammers.

The data provided by the victim can then be exploited by the criminals. For example, the personal information provided by the victim can be used to drain the customer's account balance. Although it is usually difficult to identify, there are several signs that can be used to recognize phishing scams. The main signs to watch out for in this context include: crude and unfamiliar language; phishing messages often use language that feels crude or unfamiliar. This can be the first clue indicating that something is wrong with the message. Differences in the appearance of online banking sites: when viewing a counterfeit banking website, there are sometimes differences in the site's appearance compared to the official site(Risqiana et al., 2024).

Although web icons or menu layouts may generally look similar, paying attention to small details can reveal these differences. Legal regulations regarding phishing cases involving various types of motives. Such acts are, of course, highly detrimental to customers; phishing regulations are broadly established under the legal provisions of Law No. 19 of 2016 amending Law No. 11 of 2008(Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2016).

Article 28(1): "Any person who intentionally and without authorization disseminates false and misleading information resulting in consumer loss in electronic transactions." The elements contained in Article 28(1) of the ITE Law

are the objective elements:

- The act of disseminating
- What is disseminated is false and misleading information
- From this act arises the constitutive consequence, namely consumer loss in electronic transactions.

Subjective elements:

- The element of fault, namely intentionally committing the act of disseminating false and misleading information that results in consumer loss in electronic transactions.
- Unlawful and without authorization

Article 30(1): "Any person who intentionally and without authorization or unlawfully accesses another person's computer and/or electronic system by any means."

Article 31(1): "Any person who intentionally and without authorization or unlawfully intercepts or taps electronic information and/or electronic documents within a specific computer and/or electronic system belonging to another person." Article 35 "Any person who intentionally and without authorization or unlawfully manipulates, creates, alters, deletes, or destroys electronic information and/or electronic documents with the intent to make such electronic information and/or electronic documents appear as if they were authentic data."

Article 36 of the ITE Law: "Any person who intentionally and without authorization or in violation of the law commits the acts referred to in Articles 27 through 34, thereby causing harm to another person."

Article 45A(1): "Any person who intentionally and without authorization distributes electronic information and/or documents containing content that violates public decency as referred to in Article 27(1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp 1,000,000,000.00 (one billion rupiah).

Law No. 19 of 2016 adds an explanation to Article 5, paragraphs (1) and (2), which were previously stated as "sufficiently clear"; the added explanation is Article 5,

paragraph (1) "That the existence of Electronic Information and/or Electronic Documents is binding and recognized as valid evidence to provide legal certainty regarding the operation of electronic systems and electronic transactions, particularly in matters of proof and those related to legal acts performed through electronic systems(Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2016).

Paragraph (2): "Specifically, electronic information and/or electronic documents in the form of interception, wiretapping, or recording which are part of such interception, wiretapping, or recording must be obtained for law enforcement purposes at the request of the police, the prosecution, and/or other institutions whose authority is established under the law. The Law on Electronic Information and Transactions (ITE Law) only regulates the resolution of cases by imposing criminal sanctions on persons who commit criminal acts, such as imprisonment and fines in accordance with Article 45A paragraph (1) of the ITE Law.

Criminal prosecution of offenders is considered an appropriate measure to enforce the law and serve as a deterrent; consequently, many criminal provisions in the ITE Law and the Criminal Code prescribe imprisonment and fines as penalties, as these are believed to resolve cases by deterring offenders. Therefore, the use of imprisonment and fines for offenders is considered suboptimal in ensuring victims' rights to receive material compensation, particularly in the context of cybercrime where victims' economic circumstances are vulnerable. This is also regarded as every citizen's right to receive fair legal protection.

The provisions in the ITE Law regarding searches, seizures, arrests, and detentions pose challenges for investigators because crimes in the realm of Information Technology and Electronic Transactions evolve rapidly, and perpetrators can easily conceal criminal acts or evidence (General Explanation, Paragraph 8 of Law No. 19 of 2016). To address this issue, the drafters of Law No. 19 of 2016 amended several provisions regarding criminal investigations in the field of information technology and electronic transactions as stipulated in Article 43, as explained in the final paragraph of the General Explanation.

Providing restitution to victims of cybercrime in the form of phishing is an appropriate method. This is regulated in Article 1, point 11, which states that restitution is compensation provided by the perpetrator or a third party to the victim or their family. This is also explained in Article 1, point 8 of Law No. 31 of 2014 Amending Law

No. 13 of 2006 on the Protection of Witnesses and Victims, protection is defined as actions to ensure the fulfillment of rights and provide assistance to guarantee the safety of witnesses and/or victims in accordance with applicable laws.

However, regulations regarding the protection of witnesses and victims are optional and depend on the decision of the LPSK to ensure the fulfillment of their rights. Furthermore, this law does not specify in detail the types of criminal offenses eligible for restitution, which creates uncertainty for victims. Additionally, the Criminal Code (KUHP) does not provide specific provisions for criminal compensation, and the compensation under Article 14C of the Criminal Code regarding conditional sentencing is essentially used as an alternative to avoid the principal sentence.

The imposition of specific conditions in the form of restitution in cases of conditional sentencing is solely at the discretion of the judge based on a prison sentence of up to one year or a custodial sentence, and this condition is optional.

2. The effectiveness of regulations governing phishing crimes?

Law No. 19 of 2016 on Information and Electronic Transactions. Whether or not it is effective in achieving the objectives mentioned in consideration (a), namely "to realize justice, public order, and legal certainty" in the context of electronic information and transactions, must certainly be evaluated based on specific criteria(Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2016).

The criteria used in discussing this issue are based on Lawrence M. Friedman's Theory of Legal Systems. Lawrence M. Friedman argues that the effectiveness and success of law enforcement depend on three elements of the legal system: the legal structure (structure of law), the substance of the law, and legal culture. The legal structure component of a legal system involves a number of institutions formed by that system with various functions to support its operations(Qonitatin Abidah et al., 2025).

Legal Structure (Structure of Law), according to Friedman, is referred to as the legal framework; this is the structure that provides the overall framework and boundaries. Components of the legal structure include law enforcement agencies such as the police, the prosecutor's office, the courts, and civil society organizations. As the substance of law, norms, patterns of human behavior, as well as written legal rules and the law in force within society constitute it. According to Lawrence M. Friedman, drawing on H.L.A. Hart's theory, the substance of law consists of regulations and provisions governing the behavior of an institution. Legal culture is the human attitude toward law that determines how the law is utilized, avoided, or abused(Qonitatin Abidah et al., 2025).

The effectiveness of the legal system in addressing crime in society depends heavily on the three aspects mentioned above. By mitigating potential weaknesses in these three aspects, the enforcement of criminal law in resolving criminal cases within society can achieve optimal results. The same applies to the enforcement of criminal law regarding cybercrime, where these three aspects also exert a significant influence(Putri Ramadhani Rangkuti et al., 2025).

Law enforcement plays a crucial role in the operation of the legal system. The fight against cybercrime by law enforcement agencies is closely tied to the existence of legislation, particularly laws related to information technology, especially in the context of internet-related crimes. Furthermore, when handling cybercrime cases, law enforcement officials must pay close attention to the digital evidence used by perpetrators in committing their crimes. The court requires digital evidence in cybercrime cases, as such evidence plays a crucial role in the evidentiary process during court proceedings(Nurmansyah et al., 2025).

The implementation of regulations regarding cybercrimes involving phishing techniques remains inadequate, as evidenced by the continued rise in phishing cases each year. In fact, phishing crimes are becoming increasingly rampant, targeting various banking websites, including digital banking platforms. This is due to various obstacles, including challenges in law enforcement related to understanding internet technology, the uneven distribution of technology or infrastructure, as well as socio-economic factors involving societal and cultural aspects, none of which fully support the optimal implementation of laws regarding electronic information and transactions,80 so the public perceives this as a common occurrence, and fraud and the theft of personal data are seen as easy ways to profit(Ginting, 2025).

Legislation regarding the enforcement of criminal laws against phishing is not comprehensively regulated because phishing encompasses various types of crimes, such as cybercrime, fraud, and personal data theft. The legislation governing phishing crimes is Law No. 19 of 2016 on Information and Electronic Transactions. These legal regulations serve as substantive components aimed at reducing the number of phishing attack cases. However, there are still weaknesses in these regulations. From the perspective of sanctions, there remains a lack of clarity in their application(Imelia Damai Agusthin et al., 2024).

Under the legislation, there are types of penalties imposed by judges regarding phishing crimes, such as imprisonment for a specific duration. Law No. 27 of 2022 on Personal Data Protection (PDP Law). While phishing regulations are not explicitly detailed, the existing regulations, as explained above, are sufficiently detailed, although there are still weaknesses in these rules(Yuspin et al., 2023).

Legal culture is the social mindset and social forces that determine how the law is utilized, avoided, or abused. The relationship between the era of military rule, legal culture, and public legal awareness is highly significant; the higher the level of legal awareness among the public, the more a positive legal culture will emerge. A positive legal culture has the potential to change public perceptions of the laws that have been in effect until now(Harlina Hamid & Muhammad Fadli Faisal Rasyid, 2025).

However, one of the factors influencing the effectiveness of legal protection for customers against phishing crimes in the banking sector is the culture of privacy. Evidence of the still-weak legal culture, for example, comes from several cases where people stated, "If someone contacts me, sounding so convincing as if they're from the bank and asking for data verification, I provide that verification." Evidence of Indonesia's lack of digital literacy: the majority of the Indonesian public does not yet possess a sufficiently high level of digital literacy; many people are not skilled in using technology or understanding its potential and risks(Devi Anjheli, 2025).

Cybersecurity issues: a lack of awareness regarding cybersecurity and cyberattacks can undermine the technological culture in Indonesia. From this, it can be concluded that there is low awareness of the existence of cybercrime. Digital banks provide all services and facilities digitally through online platforms. The existence of digital banking makes it easier for customers to conduct financial transactions and manage banking affairs quickly, anytime, and anywhere. When transacting, customers no longer need to interact with tellers and are not dependent on the presence of a branch office near them(Jumantoro & Firdausy, 2025).

The criteria that digital banks must meet are that banking processes must be simple, seamless, and provide convenience to customers. This allows digital banking customers to access banking services without having to visit a physical branch, so they can easily interact and connect with those closest to them simply by using a smartphone and an internet connection. As a result, digital banking has become a popular choice among various segments of society(Pian et al., 2024).

However, when you consider the effectiveness of digital banking, there is no direct interaction with customers. This actually increases the potential for phishing attacks compared to conventional banks, as it leads to a lack of awareness among the public; some customers may not be sufficiently vigilant against phishing threats and can easily be deceived by new messages claiming to come from the digital bank. To mitigate the risk of phishing attacks, digital banks must continuously educate their customers about these threats, strengthen their security measures, and actively monitor suspicious activity. Customers must also play their part by remaining vigilant, avoiding clicking on suspicious links, and refraining from carelessly disclosing personal information(Solikhah, 2025).

The effectiveness of the government's role in combating phishing in Indonesia through the Personal Data Protection Act (PDP Act). The government's role, through the Personal Data Protection Act, in combating phishing crimes in Indonesia places greater emphasis on the government's efforts to protect the public's personal data from phishing practices via the PDP Act. Although this law has been enacted, there are still many individuals and organizations that do not fully understand the Personal Data Protection Act and the preventive measures that need to be taken to protect personal data(Darnela & Rusdiana, 2025).

Since this law is still relatively new, the government needs to conduct widespread public awareness campaigns across all regions so that all government agencies, legal entities, and the public can understand their rights and responsibilities and know how to report unauthorized data collection by third parties. In today's digital age, personal data holds significant value and is often misused by irresponsible parties. Therefore, the Personal Data Protection Act is a crucial step toward ensuring privacy and individual rights regarding the collection, use, and sharing of personal data(Faisal & Zuliarti, 2024).

Based on the phishing reports discussed above, it can be said that the law is nearly effective. Why is this the case? Because, while the Personal Data Protection Act is intended to help protect customers' personal data, when its effectiveness is assessed using Lawrence M. Friedman's theory as seen in the points mentioned above it remains ineffective in terms of structure. This is evident from the continued rise in the number of phishing cases each year. In fact, phishing crimes are becoming increasingly rampant, targeting various types of banking websites, including digital banking platforms(Sulthanah & Ginting, 2025).

Law enforcement plays a crucial role in implementing the legal system. Efforts to combat cybercrime by law enforcement agencies are closely tied to the existence of legislation, particularly laws related to information technology, especially when dealing with internet-related crimes. Various challenges in the implementation of law enforcement also involve limited understanding of internet technology, uneven distribution of technology or infrastructure, and socio-economic factors(Marune & Hartanto, 2021).

The substance of non-compliance occurring in society regarding Law No. 19 of 2016 on Electronic Information and Transactions. The implementation of regulations regarding cybercrimes involving phishing techniques remains suboptimal. Regarding the legal framework, Law No. 19 of 2016 on Information and Electronic Transactions addresses phishing-related crimes. However, weaknesses persist because while legal provisions exist, enforcement officials often lack a thorough understanding of these regulations(Fauzia et al., 2021).

Legal culture and the values and attitudes that influence the implementation of the law in society are also not yet effective. For example, regarding privacy culture, there is a lack of digital literacy; the majority of the Indonesian public does not yet possess a sufficiently high level of digital literacy, and many people are not skilled in using technology or understanding its potential and risks. Cybersecurity issues, including a lack of awareness regarding cybersecurity and cyberattacks, can undermine the technological culture in Indonesia(Az-zahra et al., 2025).

ASEAN countries have already developed specific regulations regarding personal data protection. For example, Singapore began in 2012, Malaysia in 2010, the Philippines in 2012, and Thailand in 2019(Walters et al., 2019).

The EU GDPR came into effect on May 25, 2018, having a significant impact on Indonesian companies across various sectors such as transportation, e-commerce, hospitality, and other sectors that collect personal data(Wan & Ye, 2025). This should serve as a catalyst to accelerate the enactment of personal data protection regulations in Indonesia.

According to researchers from Singapore, Malaysia, Indonesia, the Philippines, Thailand, and Vietnam, of the six ASEAN countries, only Indonesia lacks a specific cybersecurity law. Regulations in Indonesia rely solely on the ITE Law. The same applies to the issue of personal data protection, for which there is no specific law. Consequently, in the event of a personal data breach, the matter is resolved through the general legal system and varies by court decision. Meanwhile, Vietnam is the only ASEAN country with comprehensive legal provisions addressing both cybersecurity and personal data protection within a single, codified law(Lestari & Mujib, 2022).

CONCLUSION

Legal regulations regarding phishing attacks that threaten the theft of customers' personal data in digital banking in Indonesia are addressed in various regulations, such as the bank's duty of confidentiality under Law No. 10 of 1998, consumer protection under Law No. 8 of 1999, and provisions related to cybercrime in Law Law No. 19 of 2016 on Information and Electronic Transactions and Law No. 27 of 2022 on Personal Data Protection. These regulations aim to provide protection for personal data and to prevent cybercrime, including phishing. Additionally, victims of cybercrime are entitled to restitution as stipulated in Law No. 31 of 2014 on the Protection of Witnesses and Victims. The establishment of a personal data protection supervisory agency, as mandated by the Personal Data Protection Law (PDP Law), is also a crucial step in strengthening Indonesia's data protection system.

However, the effectiveness of these regulations still faces various challenges when viewed through Lawrence M. Friedman's legal system theory, specifically regarding legal structure, legal substance, and legal culture. From a structural perspective, law enforcement regarding phishing cases remains suboptimal; from a substantive

perspective, there are weaknesses in the application of regulations; and from a cultural perspective, low digital literacy and public awareness of cybersecurity pose major challenges. Therefore, efforts are needed to enhance customer education, strengthen security systems, and monitor suspicious activities within digital banking services. On the other hand, more specific regulatory updates regarding phishing, along with widespread public awareness campaigns on personal data protection, are essential to improve the effectiveness of legal protection in the digital age.

REFERENCES

Akbar, M. R. (2023). Perkembangan yang Pesat dan Tantangan yang Dihadapi oleh Perbankan Digital di Indonesia. *Ecobankers : Journal of Economy and Banking*, *4*(2), 95–111. https://doi.org/10.47453/ecobankers.v4i2.989

Astutik, S., Subekti, S., Prawesti, W., Handayati, N., binti Ghapa, N., & Alifia Fernanda, M. (2025). Legal Protection of Consumer Personal Data in Digital Banking Services in Indonesia. *E3S Web of Conferences*, *657*, 07002. https://doi.org/10.1051/e3sconf/202565707002

Az-zahra, A., Marpaung, Z. A., Rohmansyah, R., & Hanan, R. A. (2025). Legal Protection against Phishing Crimes in the Banking Industry (Case Study of a State-Owned Bank). *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam*, *6*(1), 1. https://doi.org/10.58836/al-qanun.v6i1.23538

Bernanda Gunawan, A. (2024). Protection of Children Personal Data in Digital Financial Services in Indonesia. *Journal of Law, Politic and Humanities*, *4*(5), 1801–1807. https://doi.org/10.38035/jlph.v4i5.705

Candra, N., Mochtar, D. A., & Indrayanti, K. W. (2024). Banking Customer Data Security Protection in the Era of Financial Technology in Indonesia. *EAS Journal of Humanities and Cultural Studies*, *6*(03), 117–122. https://doi.org/10.36349/easjhcs.2024.v06i03.009

Darnela, L., & Rusdiana, E. (2025). Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, *14*(1), 1–28. https://doi.org/10.14421/2gg2rp29

Devi Anjheli. (2025). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(1), 165–189. https://doi.org/10.14421/990epf27

Faisal, F., & Zuliarti, W. O. (2024). The Awareness Gap in Personal Data Privacy in Indonesia's Cyberspace. *International Journal of Social Science and Human Research*, *7*(07). https://doi.org/10.47191/ijsshr/v7-i07-84

Fauzia, A., Hamdani, F., & Octavia, D. (2021). THE REVITALIZATION OF THE INDONESIAN LEGAL SYSTEM IN THE ORDER OF REALIZING THE IDEAL STATE LAW. *Progressive Law Review*, *3*(01), 12–25. https://doi.org/10.36448/plr.v3i01.46

Gana, F., Lay, E., Dethan, F. M., & Foeh, R. (2024). Service digitalization innovation model as development strategy and policy at Bank NTT Indonesia. *Journal of Infrastructure Policy and Development*, *8*(8), 3053. https://doi.org/10.24294/jipd.v8i8.3053

Ginting, L. W. (2025). The Digital Literacy for Personal Data Protection. *Sultan Agung Notary Law Review*, *7*(1), 1. https://doi.org/10.30659/sanlar.v7i1.43462

Hani Harlan. (2025). Perkembangan Financial Technology (Fintech) dalam Digital Perbankan di Indonesia. *Al-Kharaj: Jurnal Ekonomi, Keuangan & Bisnis Syariah*, *7*(5). https://doi.org/10.47467/alkharaj.v7i5.7529

Harlina Hamid, & Muhammad Fadli Faisal Rasyid. (2025). Criminal Policy in Combating Digital Banking Crime: Challenges and Prevention Strategies. *International Journal of Law and Society*, *2*(4), 95–106. https://doi.org/10.62951/ijls.v2i4.781

Ida Ayu Putu Megawati, & Ni Nengah Rupadi Kertiriasih. (2024). DAMPAK LAYANAN PERBANKAN DIGITAL TERHADAP KINERJA PERBANKAN DI INDONESIA. *JURNAL LENTERA BISNIS*, *13*(3), 1578–1591. https://doi.org/10.34127/jrlab.v13i3.1205

Imelia Damai Agusthin, Dinda Christy Nada, & Nadia Ananda Putri. (2024). Perlindungan Hukum Nasabah dari Kejahatan Phising dalam Layanan Perbankan Digital di Indonesia. *Deposisi: Jurnal Publikasi Ilmu Hukum*, *2*(4), 132–148. https://doi.org/10.59581/deposisi.v2i4.4214

Jumantoro, T. R. P., & Firdausy, M. K. (2025). Transhumanistic cybercrime analysis using a posthuman criminology approach to digital identity threats in artificial intelligence era. *Priviet Social Sciences Journal*, *5*(9), 1–16. https://doi.org/10.55942/pssj.v5i9.558

Lestari, Y., & Mujib, M. M. (2022). Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study). *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, *11*(2), 203–234. https://doi.org/10.14421/sh.v11i2.2729

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*, *2*(4), 143–152. https://doi.org/10.46336/ijbesd.v2i4.170

Nurmansyah, G., Natamiharja, R., & Setiawan, I. (2025). Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach. *Pancasila and Law Review*, *6*(1), 15–44. https://doi.org/10.25041/plr.v6i1.4138

Pian, M., Medan, K. K., & Manafe, D. R. C. (2024). Penanggulangan Tindak Pidana Cyberbullying Terhadap Anak Di Indonesia Perspektif Sistem Hukum Lawrence Meir Friedman. *Artemis Law Journal*, *2*(1), 149–162. https://doi.org/10.35508/alj.v2i1.16936

Putri, B. M. L., Rohaini, Nhung, P. H., & Putri, R. W. (2025). Analysis of Consumer Rights Protection Against the Misuse of Personal Data in Fintech Services. *Lex Publica*, *12*(1), 32–62. https://doi.org/10.58829/lp.12.1.2025.286

Putri Ramadhani Rangkuti, Muhammad Aldi Khoiri, Sumantri Ritonga, & Putri Nabila Sitorus Pane. (2025). Sanksi Pidana terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia. *Konstitusi : Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi*, *2*(3), 291–305. https://doi.org/10.62383/konstitusi.v2i3.908

Qonitatin Abidah, S., Reza Faturrahman, M., Khoirunnisa, N., Saptoadji Wicaksono, S., & Wulandari, S. (2025). Criminal Policy of Indonesian Criminal Law in Combating the Crime of Phishing. *SHS Web of Conferences*, *221*, 03006. https://doi.org/10.1051/shsconf/202522103006

Risqiana, R., Hayfa, J., Rani, R., & Wungkana, S. R. (2024). Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions. *Jurnal Penelitian*

Ilmu-Ilmu Sosial, *5*(1), 19–33. https://doi.org/10.23917/sosial.v5i1.2375

Sasea, E. M., & Sakmaf, M. S. (2023). DIGITAL BANK LEGAL CHALLENGES: SECURITY PROTECTION AND LEAKAGE OF CUSTOMER PERSONAL DATA. *Awang Long Law Review*, *6*(1), 245–250. https://doi.org/10.56301/awl.v6i1.989

Solikhah, M. (2025). Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework. *Indonesian Cyber Law Review*, *2*(1), 1–11. https://doi.org/10.59261/iclr.v2i1.15

Sriono, Risdalina, Kusno, Kumalasari M, I., & Syahyunan, H. (2024). LEGAL PROTECTION FOR DIGITAL BANK CUSTOMERS IN INDONESIA: ANALYSIS OF DATA CONFIDENTIALITY REGULATIONS AND BANK RESPONSIBILITY. *LITIGASI*, *25*(2), 301–330. https://doi.org/10.23969/litigasi.v25i2.18538

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0193

Sugihyanto, T., & Jansen Arsjah, R. (2023). The Effect of Digital Banking, Digital Transformation on the Efficiency of Commercial Banks in Indonesia. *International Journal of Islamic Education, Research and Multiculturalism (IJIERM)*, *5*(2), 387–408. https://doi.org/10.47006/ijierm.v5i2.242

Suharbi, M. A., & Margono, H. (2022). Kebutuhan transformasi bank digital Indonesia di era revolusi industri 4.0. *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan*, *4*(10), 4749–4759. https://doi.org/10.32670/fairvalue.v4i10.1758

Sulthanah, M. Y., & Ginting, R. (2025). Analisis Problematika Penegakan Hukum Terhadap Tindak Pidana Perjudian Online di Indonesia. *Jembatan Hukum : Kajian Ilmu Hukum, Sosial Dan Administrasi Negara*, *2*(2), 01–15. https://doi.org/10.62383/jembatan.v2i1.1438

Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Pub. L. No. 11 (2024).

Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Pub. L. No. 19 (2016).

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. 27 (2022).

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. 27 (2022).

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. 27, Indonesia, Pemerintah Pusat (2022).

Undang-Undang (UU) Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Pub. L. No. 8 (1999).

Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature Singapore. https://doi.org/10.1007/978-981-13-8110-2

Wan, G., & Ye, X. (2025). East Asian Personal Data Protection Laws and International Medical Data Sharing: Pathways for Coordination. *International Journal of Multidisciplinary Research and Growth Evaluation*, *6*(5), 109–113. https://doi.org/10.54660/.IJMRGE.2025.6.5.109-113

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1), 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130