The Legal Protection Regarding Consumer Losses in Banking Transactions Caused by Phishing

Rani Apriani
Universitas Singaperbangsa Karawang, Indonesia
Corresponding Email: rani.apriani@fh.unsika.ac.id

Article Info

Received: 2025-02-02
Revised: 2025-02-21
Accepted: 2025-03-27

Keywords:
Banking, Consumer, Legal Protection, Phishing.

Abstract

This study is a normative legal study with a conceptual and legislative approach. The results of the study confirm that legal protection that includes the bank's obligation to maintain data security and provide preventive education is very necessary, along with legal resolution of problems if losses occur due to phishing. Strengthening regulations and supervision from the government, the Financial Services Authority (OJK), and banking is very important to minimize the risk of phishing and protect customers effectively. In this case, the bank's legal accountability is key to providing legal certainty and protecting the rights of the injured party, with the condition that the bank can only be held accountable if it is proven negligent in managing data and system supervision. Banks can actually be held accountable either civilly or criminally according to the type and level of the bank's error. This study recommends strengthening stricter regulations, improving data security systems by banks, and providing more comprehensive preventive education to customers regarding potential phishing risks, to ensure optimal protection and minimize potential losses.

I. Introduction

The increasingly rapid and complex progress of technology and information has also had an impact on the dynamics of crime. (Butler et al., 2024). Along with these developments, the modus operandi of crime has also undergone a transformation, including in terms of the use of technology and information as a means to carry out criminal acts. (Anggono & Riskiyadi, 2021). The type of crime involving technology and information systems is known as cybercrime, which not only follows the development of information technology but also utilizes computer-based devices as the main medium in its implementation. (Milla Mudzalifah, 2023)(Prasetio, 2024).

Phishing is a type of cybercrime that has grown alongside advancements in technology. It's a digital crime aimed at obtaining sensitive information or data from victims, often through emails, social media posts, or text messages. (Muhammad & Harefa, 2023). The term "phishing" originates from the English word "fishing," where in this context, victims are "lured" into accessing a specific link and providing personal information such as usernames and passwords. (Gulo et al., 2021).

Phishing perpetrators generally pretend to be official parties or institutions to deceive victims. (Odie et al., 2022). Phishing perpetrators embed malicious links in messages designed to appear legitimate, aiming to trick victims into accessing these phishing links. (Gulo et al., 2021). Phishing targets personal data (name, age, address), account data (username and password), and financial data (credit card or bank account numbers). This stolen data can be used for further criminal activities, such as account misuse or financial fraud.

Technically, a phishing attack begins with target selection and the development of a data-gathering strategy. The perpetrator then creates a fake email or webpage mimicking a legitimate entity. Once the victim enters personal data through this fake medium, the perpetrator accesses and monitors the provided information, using it for illegal activities such as unauthorized purchases or other fraudulent actions.

That's correct. The statement indicates that between January 2017 and early December 2020, the Indonesian National Cyber and Crypto Agency (BSSN) received 12,538 reported cybercrimes via one of its platforms, likely

"Patrolisiber.". (Frensh, 2021). Of that number, only 6,694 cases were successfully resolved, with total losses estimated at IDR 1.17 trillion. (Lestari & Mujib, 2022). Of the total reports, 5,477 cases were reported as online fraud, 802 cases of illegal access, 317 data theft cases, 244 cases of electronic system hacking, and 331 cases of data manipulation, in addition to numerous other cases spread across various sectors. (Gobel, 2021).

One prominent case involved debit card information theft through skimming techniques in early 2018. This attack targeted 64 banking institutions globally, including 13 national banks in Indonesia, both government-owned and private. The banks incurred losses of Rp18 billion due to having to reimburse stolen funds to customers. Phishing is a form of cyber fraud aimed at obtaining personal and sensitive information from customers, such as user IDs, passwords, PINs, account numbers, or credit card data, by impersonating official entities - usually banks - through emails, text messages, fake websites, or other electronic media. Phishing perpetrators (phishers) use psychological manipulation techniques to trick victims into voluntarily providing their personal data, which is then used to access and hack into the victim's bank accounts. Phishing poses a serious threat to digital banking transactions, leading to financial losses and data breaches for customers. Preventing and addressing phishing requires collaboration between banks, regulators, and customers, as well as strict law enforcement to protect security and trust in digital banking services.

According to Article 37B paragraph (1) of Law No. 10 of 1998 concerning Amendments to Law No. 7 of 1992 concerning Banking (Banking Law), every bank has an obligation to guarantee funds deposited by customers at the institution. To prevent and protect customers from potential losses due to electronic banking services, reference can be made to Article 29 paragraph (4) of the Banking Law, which obliges banks to provide information about potential risks associated with transactions conducted by customers. This provision is reinforced by Article 29 paragraph (1) of Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection, which states that every service provider must maintain the security of consumer assets under their responsibility. This provision is essentially in line with Article 2 of Law No. 8 of 1999 concerning Consumer Protection (Consumer Protection Law), which states that one of the important principles in consumer protection is the principle of consumer safety and security. Furthermore, Article 42 paragraph (1) of Bank Indonesia Consumer Protection also stipulates that service providers are

responsible for customer losses caused by errors, negligence, or actions that contradict laws and regulations, whether committed by the board of directors, board of commissioners, management, employees, or third parties representing or working for the benefit of the service provider.

However, according to Article 42 paragraph (2) of these regulations, if the service provider can prove that the loss occurred due to the customer's own error or negligence, then the responsibility for the loss is not borne by the service provider. Forms of service provider liability for customer losses may include compensation, restoration of reputation, or other forms of liability. However, these regulations do not explicitly clarify the form of bank liability if customer losses are caused by phishing attacks. This is because, in practice, losses due to phishing can occur both due to customer negligence in maintaining their personal information and due to bank negligence in optimally protecting customer data.

Based on the legal issues outlined above, this study focuses on answering two questions: (i) the regulation of legal protection for customers related to phishing threats in banking practices and (ii) the efforts of legal accountability provided for customers related to phishing threats in banking practices.

2. Research Method

This research is a normative legal study, focusing on the examination of doctrinal legal materials. Normative legal research involves a literature review of authoritative legal documents, such as legislation and court decisions. (Marzuki, 2017). The legal materials are analyzed qualitatively using legal principles, legal theories, and legal concepts to find answers to the legal issues being studied. In implementing this research, two approaches were used, namely the statute approach and the conceptual approach. The statutory approach is carried out by examining all regulations and laws that are relevant and directly related to the issues that are the main problem of the research. Meanwhile, the conceptual approach is used to understand the principles and legal principles that have developed in legal science, which are obtained from the thoughts of experts and legal doctrines to strengthen the analysis of the legal issues being studied. The primary legal materials used in this study consist of: (i) Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking (Banking Law), Law Number 8 of 1999 concerning Consumer Protection (PK Law), and Bank Indonesia Regulation

Number 3 of 2023 concerning Bank Indonesia Consumer Protection. Secondary legal materials, in the form of literature that supports and explains primary legal materials, such as books, scientific articles, legal journals, and other relevant sources. Non-legal materials, namely supporting materials such as legal dictionaries used to clarify technical terms in legal studies. The collection of legal materials is carried out through the library research method.(Irwansyah, 2020). This technique involves reading, analyzing, and examining various library sources and media directly related to the legal issues at the heart of the research. The collected legal materials are processed through systematic stages: inventory, identification, classification, and systematization. (Ali, 2009). The goal of systematization is to organize the legal materials in a structured way to avoid contradictions between legal norms. Once systematically organized, the legal materials are analyzed using the statutory approach, the conceptual approach, and the case approach to formulate answers to the research questions

3. Results and Discussion

Customer Protection Arrangements Regarding Phishing Threats in Banking Practices

Customers in the context of banking are parties who use bank services, either as depositors (depositing customers) or as recipients of credit facilities (debtor customers).(Puspasari, 2020). In practice, bank customers are consumers of banking services because banks provide financial products and services consumed by the public. The relationship between a bank and its customer is based on an agreement or contract, typically a standardized contract.(Hidayat, 2020). In this agreement, the bank is usually in a more dominant position because all the provisions and clauses have been prepared unilaterally by the bank. (Dauri & Waliyyatunnisa, 2020). Customers are presented with a "take it or leave it" scenario, meaning they have no choice but to accept the entire agreement as it is or decline the service altogether. This puts customers in a weaker position compared to banks. (Rachmaniyah & Wahyoeno, 2022).

The Consumer Protection Law (UU PK) recognizes bank customers as consumers entitled to legal protection. The UU PK provides a legal basis for customers to address potential losses resulting from unfair banking practices, particularly concerning the use of standardized clauses in contracts. (Mahmudah et al., 2023). Perlindungan ini meliputi hak atas pelayanan yang nyaman, aman, dan selamat dalam menggunakan produk dan jasa bank (Sulistyowati, Eny, Muh. Ali Masnun, 2025). In a standard agreement, the customer's position as a consumer tends to be weak because the customer is not free to determine the contents of the agreement, all clauses have been determined unilaterally by the bank. (Dauri & Waliyyatunnisa, 2020). Many clauses in standardized contracts prioritize the interests of the bank as creditor, rather than the customer as debtor. This imbalance in bargaining power often leads to disadvantages for the customer. (Hidayat, 2020).

Legal protection in the banking sector is based on several theories and principles that form the basis for guaranteeing customer rights and maintaining public trust in banking institutions. There are several theories, namely(Widayanti, 2022):

1. Absolute Bank Secrecy Theory: This theory states that banks have an absolute duty to maintain the confidentiality of customer information

without exception. Any violation of bank secrecy results in legal liability for the bank.

2. Relative Bank Secrecy Theory: This theory allows banks to disclose customer secrets under certain legal circumstances, such as a court order or for the purpose of broader legal protection.
3. Consumer Protection Theory: Bank customers, as consumers of banking services, are entitled to legal protection under the Consumer Protection Law (UU PK). This theory positions banks as business entities obligated to provide transparent, honest information and serve customers in good faith. This protection aims to ensure legal certainty and prevent customer losses due to unfair banking practices.
4. Legal Liability Theory: Banks, as legal entities, are responsible for their legal actions, especially if they cause harm to customers. This theory emphasizes that banks are legally accountable for any violations they commit, unless there are grounds for exemption from liability.
5. Prudential Principle Theory: In the context of banking, the prudential principle is a fundamental theory of legal protection that requires banks to conduct their business with utmost care and strict supervision by authorities such as Bank Indonesia and the Financial Services Authority (OJK). This aims to ensure the continuity of banks and protect customers from the risk of bank failures.
6. Deposit Guarantee Theory: This theory relates to the establishment of deposit guarantee institutions that protect customer funds if a bank fails. This is an explicit form of protection that provides customers with peace of mind when depositing their funds in banks.

Generally, theories of legal protection in banking combine several approaches: maintaining absolute or relative customer confidentiality, ensuring customer rights as consumers through transparency and fair service, enforcing bank legal liability for customer losses, implementing the prudential principle and strict supervision to maintain bank stability, and guaranteeing customer deposits through deposit guarantee institutions. (Prayuti, 2023). These theories work together to create a comprehensive system of legal protection for banking customers.

Given the various legal protections in banking, there is an urgent need to regulate and formulate measures to protect customers, particularly when they

experience phishing attacks. Phishing is a cybercrime that aims to steal personal information and financial data from customers through deceptive methods, such as sending emails, messages, or creating fake websites that resemble legitimate banks. These scams trick victims into entering sensitive data like usernames, passwords, PINs, and OTP codes. (Muhammad & Harefa, 2023). There are several customer losses caused by phishing, such as customers can lose funds directly if banking data is successfully stolen and misused by phishing perpetrators to carry out unauthorized transactions. (Amin Muftiadi, Tri Putri Mulyani Agustina, 2022). In addition, data such as account numbers, credit cards, and other personal information can be stolen and used for further crimes. Non-financial losses can occur in the form of decreased customer trust in the security of digital banking services, which has an impact on the bank's reputation and customer comfort in using e-banking services.

The position of customers as consumers in banking transactions is legally recognized and protected by law. However, in practice, the position of customers is still weaker than banks because of the dominance of banks in the preparation of standard agreements. Therefore, effective legal protection and enforcement of regulations are very important to guarantee the rights of customers as consumers of banking services (Anggara & Warsifah, 2022). Legal protection for customers as banking consumers is regulated through two mechanisms, namely preventive efforts in which banks regulate the procedures for including standard clauses and the bank's obligation to provide clear and transparent information to customers, as stipulated in Article 18 of the PK Law. Repressive efforts, namely when there is a resolution of disputes and customer complaints against the bank, either through the bank's internal mechanism or an external dispute resolution institution, as stipulated in Bank Indonesia Regulation Number 3 of 2023 concerning Bank Indonesia Consumer Protection.

In general, banks can try to take legal protection steps to anticipate phishing, such as Banks are required to apply the principle of confidentiality and security of customer data with preventive measures, such as educating

customers on how to avoid phishing and strengthening digital security systems. Repressive efforts include resolving problems through legal processes and supporting customers who are victims of phishing to minimize losses. This also includes that the Bank needs to provide complaint services and conduct investigations into phishing cases that befall customers.

.

Legal Accountability Efforts Given to Customers Relating to Phishing Threats in Banking Practices

Phishing is a fraudulent method that aims to obtain someone's personal information through deceptive means. Data that is often targeted by phishing includes personal information such as name, age, and address, account data such as username and password, and financial data such as credit card information and account numbers. (Purwanti et al., 2023). The official term used for this technique is phishing, which comes from the English word "fishing", which means fishing. (Aryono & Barkhuizen, 2021). The primary goal of phishing is to trick individuals into unknowingly revealing their personal data, intending to use this information for criminal activities.

Phishers typically impersonate legitimate authorities, using fake websites or emails designed to appear authentic, thus trapping many victims. Data obtained through phishing can be used directly for fraud or sold to others for misuse, such as account takeover. According to data from the Directorate General of State Assets, approximately 32% of data theft cases involve phishing. Furthermore, at the beginning of 2020, the Anti-Phishing Working Group recorded over 165,000 phishing websites with the potential to deceive victims. (Amin Muftiadi, Tri Putri Mulyani Agustina, 2022).

Types of phishing that are often encountered include (Odie et al., 2022):

a. Email Phishing

As the name suggests, this type of phishing uses email to reach victims. Around 3.4 billion fraudulent emails are sent daily as part of phishing attempts.

b. Spear Phishing

This is a more targeted variant of email phishing. Unlike regular phishing, which sends emails randomly to many people, spear phishing targets

specific individuals after gathering basic information about the victim, such as their name and address.

c. Whaling

This type of phishing is even more specific, targeting high-profile individuals within an organization, such as company owners, directors, or HR managers. Successful whaling can provide perpetrators with highly valuable access.

d. Web Phishing

Web phishing involves creating fake websites that mimic legitimate sites to deceive potential victims. These phishing sites use domain names very similar to the original site, a technique known as domain spoofing.

Given the prevalence of phishing attacks, legal accountability is crucial. Legal liability refers to the obligation of an individual to bear the consequences of their unlawful actions, whether in the form of penalties or compensation. (Anggraeny & Tongat, 2020). This concept is closely linked to rights and obligations, where one person's rights are paired with another's obligations. If these obligations are violated, legal liability arises. According to Hans Kelsen, a person is legally liable when they are subject to sanctions as a result of actions that violate legal rules. (Jimly Asshidiqie, 2012)(Harun, 2019). In general, the theory of legal liability serves to provide legal certainty, uphold justice, and protect the rights of those harmed by unlawful acts. Legal liability encourages legal subjects to act according to the rules and to take responsibility for the consequences of their actions. (Milik & Pilarski, 2023). In short, the general theory of legal liability asserts that a person can be held accountable for unlawful acts, whether or not there is fault, with the goal of upholding justice and providing legal protection to the harmed party. (Milik & Pilarski, 2023).

This legal responsibility is often referred to as liability, which means responsibility for mistakes made by legal subjects. (Ershova & Feyzrakhmanova, 2022). In general, legal liability can be divided into several types based on the element of fault and the nature of responsibility, namely:(Aqil et al., 2022):

a. Fault-Based Liability: An individual is responsible for violations committed intentionally or through foreseeable negligence that causes harm to another party.
b. Strict Liability: An individual is responsible for their actions regardless of intent or negligence. This principle asserts that a person can be held

liable even if they are not at fault.

c. Liability Without Fault: Responsibility arises without proof of fault, such as in cases of specific risks governed by law.

Legal liability in banking has unique characteristics that distinguish it from other legal fields, given the nature and function of banks as institutions that collect public funds and conduct highly sensitive business activities. Banks are obligated to be responsible for losses suffered by customers due to errors or negligence by bank employees in performing their duties. (Tulus Prijanto, 2020). This is based on the principle that a bank, as a corporation, is responsible for the actions of those under its employ (vicarious liability), as stipulated in Article 1367 of the Indonesian Civil Code (KUHPerdata). (Weriansyah & Ramadani, 2022). Civilly, banks are obliged to provide compensation to customers if financial losses occur due to negligence or unlawful actions of bank employees. (Prayuti, 2023). Criminally, liability can only be imposed on individuals such as directors, commissioners, or bank employees who commit banking crimes, not on the bank as a corporation.

A bank's liability arises from the contractual relationship between the bank and its customers. Without a contractual relationship, no legal liability can be imposed on the bank, except in cases of unlawful acts meeting specific elements. Banks have a duty to conduct their business with prudence and strict supervision of employees and internal procedures to prevent customer losses. (Subekti, 2023). Failure to uphold this principle can lead to legal liability. A bank can be held strictly liable for losses caused by its employees, without having to prove direct fault on the part of the bank itself. This refers to the theory of vicarious liability, which states that a bank is responsible for the actions of employees under its supervision. (Wandani Syahrir, Sabir Alwy & Fakultas, 2023).

Banks are liable not only for their own actions but also for the actions of employees or other parties acting within the scope of their duties and authority that harm customers. A bank can be held legally liable for customer losses due to phishing, but this liability is limited depending on the bank's negligence. If a customer's loss is due to bank negligence—for example, failure to promptly act

on a customer report to block an account after a phishing attack—the bank can be held liable for damages. However, if the loss is due to customer negligence (e.g., willingly providing personal data to a phisher) or force majeure, the bank is usually not liable. Therefore, bank liability balances protecting customers and holding them accountable for preventing phishing attacks.

Regarding phishing attacks, a bank can also face criminal liability if it lacks adequate security systems or is negligent regarding security, leading to phishing. This is in accordance with Article 30 paragraph (1) and Article 46 of the Indonesian ITE Law (Information and Electronic Transactions Law), which governs unauthorized illegal access to another person's electronic system, relevant to phishing. In this context, a bank lacking security or displaying negligence leading to phishing that harms customers can be considered in violation of Article 30 paragraph (1) and Article 46 of the ITE Law. However, for criminal liability, the customer needs to provide evidence of the lack of security or bank negligence leading to the phishing attack.

Customers experiencing losses due to phishing can take several legal steps: reporting to the bank to immediately block the account and conduct an investigation; if a direct settlement with the bank is unsatisfactory, filing a complaint with the Financial Services Authority (OJK) for mediation; and if there is still no resolution, filing a civil lawsuit in court to hold the bank accountable. Indonesian court decisions have shown that banks can be held liable if proven negligent, such as in the Makassar District Court Decision Number 248/Pdt.G./2023/PN Mks, which penalized a bank for not promptly addressing a customer's complaint about phishing.

In summary, legal liability for phishing is crucial for legal certainty and protecting the rights of victims. The concept of legal liability, involving individual obligations and rights, requires those violating the law to bear the consequences of their actions, whether through penalties or compensation. In the context of phishing, banks, as institutions managing public funds, are responsible for customer losses resulting from negligence in fulfilling their

obligations, such as failing to secure customer data or address phishing complaints. Banks can be held legally liable through vicarious liability, meaning the bank is responsible for its employees' actions. However, if the loss is due to customer negligence (e.g., disclosing personal information to a phisher), the bank is not liable. Customers have the right to claim compensation through internal bank complaints, the OJK, or the courts, with the bank only being liable if proven negligent in data management and protection. This legal responsibility aims to balance protecting customers and upholding their obligation to prevent phishing attacks.

4. Conclusion

The Phishing is a serious threat to digital banking transactions, potentially causing financial and non-financial losses for customers. Legal protection for customers includes the bank's obligation to maintain data security, provide preventative education, and offer legal recourse if losses occur due to phishing. Strengthened regulation and oversight from the government, OJK (Financial Services Authority), and banks are crucial to minimize phishing risks and optimally protect customers. Legal accountability for phishing cases is essential for legal certainty and protecting the rights of harmed parties. Banks, as institutions managing public funds, are responsible for customer losses due to negligence in data management and system oversight. However, banks are only liable if proven negligent; losses due to customer negligence are not the bank's responsibility. Accountability can be civil or criminal, depending on the type and nature of the bank's error. Therefore, balancing the bank's obligation to protect customers and the customer's obligation to safeguard their personal data is crucial.

Recommendations for addressing phishing threats in digital banking include stricter regulation from the government and OJK to ensure optimal customer protection. Banks need to improve data security systems and provide more comprehensive preventative education to customers about potential phishing risks. Furthermore, banks should be more proactive in monitoring transactions

and identifying potential threats early to minimize potential losses.

Refrences

Ali, Z. (2009). *Metode Penelitian Hukum*. Sinar Grafika.

Amin Muftiadi, Tri Putri Mulyani Agustina, M. E. (2022). Studi kasus keamanan jaringan komputer: analisis ancaman phisingterhadap layanan online banking. *Hexatech: Jurnal Ilmiah Teknik*, *1*(2), 60–65.

Anggara, B. J., & Warsifah, W. (2022). Penerapan Hukum Kepailitan dalam Kaitannya Kedudukan Otoritas Jasa Keuangan (OJK) sebagai Institusi Pengatur dan Pengawas Perusahaan Asuransi Negara (Contoh Kasus PT. Asuransi Jiwasraya). *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *5*(4), 1250–1259. https://doi.org/10.54371/jiip.v5i4.555

Anggono, A., & Riskiyadi, M. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review. *Jurnal Manajemen Dan Organisasi (JMO)*, *12*(3), 239–251.

Anggraeny, I., & Tongat, T. (2020). Notary Liability over their Involvement in Document Falsification Crime. *Varia Justicia*, *16*(1), 31–38. https://doi.org/10.31603/variajusticia.v16i1.3307

Aqil, N. A., Putri, C. M., & Yunisa, D. (2022). Evaluation Of Cash On Deivery System For Improving Legal Certainty In The Development Of Electronic Transactions In Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *2*(2), 251–264. https://doi.org/10.15294/ipmhi.v2i2.55074

Aryono, & Barkhuizen, J. (2021). Criminal law enforcement of Phising attacks on online banking services. *International Conference Health, Science And Technology (ICOHETECH)*, 360–363. http://ojs.udb.ac.id/index.php/icohetech/article/view/1160

Butler, S., Maglione, G., & Buchan, J. (2024). Institutionalising restorative justice for adults in Scotland: An empirical study of criminal justice practitioners' perspectives. *Criminology and Criminal Justice*, *24*(1), 269–290. https://doi.org/10.1177/17488958221104229

Dauri, D., & Waliyyatunnisa, N. (2020). Akibat Hukum Terhadap Penerapan Klausula Eksonerasi Dalam Perjanjian Baku. *Humani (Hukum Dan Masyarakat Madani)*, *10*(1), 97–111.

Ershova, I. V., & Feyzrakhmanova, D. R. (2022). Medical Applications of Artificial Intelligence (Legal Aspects and Future Prospects) Vasiliy. *Laws*, *11*(3), 6.

Frensh, W. (2021). Penanggulangan Tindak Pidana Siber Dengan Menggunakan Teori Jendela Pecah. *Doktrina: Journal of Law*, *4*(2), 159–169. https://doi.org/10.31289/doktrina.v4i2.5793

Gobel, T. (2021). *Data Penanganan Kasus Kejahatan Siber di Patrolisiber.id kok Mandek di Mei 2020?* https://cyberthreat.id/read/10925/Data-Penanganan-Kasus-Kejahatan-Siber-di-Patrolisiberid-kok-Mandek-di-Mei-2020.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Pampas: Journal of Criminal Law: Journal of Criminal Law: Journal of Criminal Law*, *1*(2), 68–81.

https://doi.org/10.22437/pampas.v1i2.9574
Harun, M. (2019). Philosophical Study of Hans Kelsen ' s Thoughts on Law and Satjipto Rahardjo ' s Ideas on Progressive Law. *Walisongo Law Review (Walrev)*, *1*(2), 195–220. https://doi.org/10.21580/Walrev/2019.1.2.4815
Hidayat, M. S. (2020). Penyalahgunaan Klausula Eksonerasi Yang Merugikan Konsumen. *Jurnal Juristic*, *1*(01), 107. https://doi.org/10.35973/jrs.v1i01.1487
Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode dan Praktik Penulisan Artikel* (3rd ed.). Mira Buana Media.
Jimly Asshidiqie, M. A. S. (2012). *Teori Hans Kelsen Tentang Hukum* (1st ed.). Konstitusi Press.
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. https://doi.org/10.14421/sh.v11i2.2729
Mahmudah, S., Asadullah, M. O. H., Al, H., & Arie, A. S. Y. (2023). Consumer Protection Arrangements For Flat Houses In The Bankruptcy Regulation Regime In Indonesia. *Russian Law Journal*, *11*(6), 291–303.
Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi* (13th ed.). KENCANA.
Milik, P., & Pilarski, G. (2023). Cyberattacks and the bank ' s liability for unauthorized payment transactions in the online banking system – theory and practice. *Cybersecurity and Law*, *1*(9), 109–112.
Milla Mudzalifah, P. (2023). The Politics Of Criminal Law In Cybercrime: An Efforts To Combat Information Technology Crimes In Indonesia. *Pembaharuan Hukum*, *10*(1), 79.
Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web tindakan dan perbuatan hukum yang nyata . Secara yuridis dalam hal ruang cyber. *USM Law Review*, *6*(1), 226–241.
Odie, I. K., Putra, K., Darmawan, I. M. A., & Juliana, I. P. G. (2022). Crime Actions In The Digital World In The Form Of Phising. *CyberSecurity and Digital Forensics*, *5*(2), 77–82.
Prasetio, D. E. (2024). Politik Hukum Omnibus Law Terkait Cybercrime di Indonesia dalam Perspektif Hukum Progresif. *Indonesian Journal Of Law Studies*, *3*(1), 27–41.
Prayuti, Y. (2023). Restrictions on Cross-Border Trade in E-Commerce as a Form of Consumer Protection. *JILPR Journal Indonesia Law and Policy Review*, *5*(1), 144–156. https://doi.org/10.56371/jirpl.v5i1.177
Purwanti, Y., Rachman, F., Gunawan, T., & Kartadinata, A. (2023). Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung. *Audi Et AP : Jurnal Penelitian Hukum*, *2*(1), 64–71. https://doi.org/10.24967/jaeap.v2i01.2088
Puspasari, S. (2020). Perlindungan Hukum bagi Investor pada Transaksi Aset Kripto dalam Bursa Berjangka Komoditi. *Jurist-Diction*, *3*(1), 303. https://doi.org/10.20473/jd.v3i1.17638
Rachmaniyah, S., & Wahyoeno, D. (2022). Perjanjian Baku Yang Memuat Klausula Eksonerasi Dalam Perspektif Hukum Perlindungan Konsumen. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, *2*(2), 714–724.

https://doi.org/10.53363/bureau.v2i2.100

Subekti, S. (2023). Pentingnya Bentuk Akta Notaris Dalam Akta Perbankan Syari'ah Terhadap Perlindungan Hukum Pada Nasabah (Muhil) Yang Berkeadilan Di Indonesia. *Jurnal Pro Hukum*, *12*(3), 832–841.

Sulistyowati, Eny, Muh. Ali Masnun, D. E. P. (2025). Arrangements for online food delivery service drivers to achieve food safety. *IOP Conf. Series: Earth and Environmental Science*, *1454*(1), 1–7.

Tulus Prijanto, M. T. (2020). Hukum Bisnis Terhadap Perdagangan Internasional Era Globalisasi Sebagai Perlindungan Eksportir, Importir, Dan Investor. *Ilmu Manajemen Dan Akuntansi Terapan*, *11*(November), 258–270.

Wandani Syahrir, Sabir Alwy, I., & Fakultas. (2023). Tanggung Jawab Hukum Perdata Terhadap Tindakan Malapraktik Tenaga Medis. *Amanna Gappa*, *31*(1), 64–76.

Weriansyah, A., & Ramadani, A. P. (2022). The Analysis of Corporate Crime in Indonesia's Intellectual Property Laws. *Global Legal Review*, *2*(1), 53. https://doi.org/10.19166/glr.v2i1.5139

Widayanti, P. W. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Legacy : Jurnal Hukum Dan Perundang-Undangan*, *2*(2), 4.