 p-ISSN: 2548-9267 | e-ISSN : 2549-2365, Open Access at : *http://unramlawreview.unram.ac.id/index.php/ulrev*

Legal Protection of Consumers from Personal Data Security Risks, Threats of Fraud and Phishing (Cybercrime) in E-Wallet Payment Systems

Yuyut Prayuti
Nusantara Islamic University
prayutiyuyut@gmail.com

Arman Lany
Nusantara Islamic University
arman_lany@yahoo.com

Yohan Edward Marpaung
Nusantara Islamic University
johan.edward.m@gmail.com

Elmend Lorentzon
Nusantara Islamic University
lorentzoni@gmail.com

ABSTRACT.

In the era of financial technology, e-wallets have become a popular payment tool among e-commerce users aged 19-45. However, e-wallets face security issues, such as breach cases that harm users. Regulations such as PBI Number 20/6/PBI/2018 and POJK No. 6/POJK.07/2022 requires organizers to ensure security and consumer protection, but their implementation could be better. This study aims to 0061nalyze the legal protection of consumers from the risk of personal data security, the threat of fraud, and circumvention (cybercrime) in the e-wallet payment system. The method used in this research is normative research. Based on the principle of legality, cybercrimes such as data theft have violated the ITE Law. Therefore data must be protected according to the Ministry of Communication and Information and Bank Indonesia Regulations. According to Philipus M. Hadjon's theory of legal protection, , preventive and repressive measures are needed to overcome legal problems such as data theft on e-wallets.

Keywords:Cybercrime, E-Wallet Payment System, Legal Protection.

INTRODUCTION

As time goes by, cash is no longer the only means of payment. In the current era, the financial system has entered the era of financial technology. Referring to the 2016 Bank Indonesia Regulation number 18/40/PBI/2016, the electronic service for storing instrument data is an e-wallet. Cards and electronic money are payment instruments that can hold funds to make payments.[1]Based on research results regarding the use of e-wallets, it is clear that active e-commerce users are aged 19-45 years. This is also proven by the highest market penetration achieved by ShopeePay (68%), followed by OVO (62%), DANA (54%), GoPay (53%), and

[1]Muhammad Taufik Hidayat, Qurrotul Aini, and Elvi Fetrina, "User Acceptance of E-Wallet Using UTAUT 2 (Case Study)," National Journal of Electrical Engineering and Information Technology (2020).

DOI: https://doi.org/10.29303/ulrev.v8i2.354

LinkAja (23%).[2] From June 2019 to June 2020, analysis results on using financial applications in Indonesia showed an up to 70% increase. Total sessions in 2019 for the use of financial applications were 1.67 billion, increasing to 2.83 billion as of June 2020.[3]

As a system created by humans, e-wallets have shortcomings that often make users feel uneasy. This unrest was triggered by the emergence of various cases related to e-wallets. Reporting from KONTAN.CO.ID, Mr Sarjono, a digital wallet user, lost 2.1 million in cash due to an e-wallet hack carried out by individuals through the marketplace.[4] Another case was also experienced by an Indonesian artist named Aura Kasih, who lost 11 million in a digital wallet application, and the loss experienced by an OVO user was 1.5 million due to the balance suddenly disappearing.[5,6] If this continues, there will be more and more misuse of e-wallets leading to an increase in cybercrime cases.

Losing balance in an e-wallet is one of the problems that users worry most about. This is not without reason; Technical errors, acts of cybercrime, or other external interference may result in financial losses for users who report problems, often get less than satisfactory responses. Slow response, complicated claims procedures, and sometimes failure to recover lost funds. Financial Services Authority (OJK) Regulation No. 6/POJK.07/2022, there is an obligation for Financial Services Business Operators (PUJK) to ensure the integrity and security of the information technology they use, as well as the protection of consumers' data and information. These cases are a strong signal for services to improve their security systems and provide more effective and faster problem-resolution mechanisms.[7]

In addition, the effectiveness of e-wallet security systems is being questioned. But it's not just the security system, regulations also play an essential role. In PBI Number 20/6/PBI/2018, in Chapter IV concerning the Administration of Electronic Money, Article 34 paragraph (1) letter b states, "In administering Electronic Money, Operators are obliged to implement information system security standards". It is also regulated in Article 34 paragraph (2) letter b that "In addition to fulfilling the obligations as intended in paragraph (1), specifically for Operators in the form of Publishers, they must apply the principles of consumer protection."[8]Apart from that, PBI Number 20/6/PBI/2018 also includes regulations regarding compensation for financial losses, but they have not been regulated clearly and in detail, which makes the lack of clarity in this regulation give rise to different interpretations between one institution and another, resulting in compensation for losses. This financial situation coul be better.[9] Related to several cases and regulations governing security systems above, this has motivated researchers to analyze the legal protection of consumers from personal data security risks, fraud threats and cybercrime in e-wallet payment systems.

---

[2]Roland Fran Vernando et al., "Level of Effectiveness of Regulations and Security Systems in Reducing E-Wallet User Anxiety," Journal of Buana Akuntansi (2022).

[3]Vivin Dian Devita, "Local E-Wallets Still Dominate Q2 2019-2020," IPRICE, last modified 2020, accessed March 12, 2024, https://iprice.co.id/trend/insights/top-e-wallet-di -indonesia-2020/.

[4]Shifa Nur Fadila and Yudho Winarto, "Rapid Cases of Hacking on DANA Digital Wallets, Here's DANA's Response," Kontan.Co.Id, last modified 2023, https://keuangan.kontan.co.id/news/marak-kas-pembobolan -on-digital-wallet-funds-this-is-the-fund response.

[5]Indiana Malia, "Aura Kasih balance lost IDR 11 million, important! Check BI Rules Regarding E-Wallets," IDN Times, last modified 2019, accessed March 24, 2024, https://www.idntimes.com/business/economy/indianamalia/saldo-aura-kasih-raib-rp11-juta- important-check-the-rules-about-e-wallet.

[6]Muchammad Fahryan Putra and Lucky Dafira Nugroho, "Legal Protection of Electronic Wallet Users for the Loss of Electronic Money," PROHUTEK Proceedings of the National Seminar on Law and Technology (2020).

[7]Roland Fran Vernando et al., "Level of Effectiveness of Regulations and Security Systems on Reducing E-Wallet User Anxiety."

[8]Cecilia Michell et al., "Systematic Literature Review of E-Wallet: The Technology and Its Regulations in Indonesia," in 2022 International Conference on Information Technology Systems and Innovation, ICITSI 2022 - Proceedings, 2022.

[9]Ni Desak Made Eri Susanti, Ida Bagus Putra Atmadja, and AA Sagung Wiratni Darmadi, "Legal Protection for Owners of E-Money Issued by Banks in Non-Cash Transactions," Kertha Semaya: Legal Science Journal (2019).

Based on the explanation above, the formulation of the problem in this research arises, namely, how to enforce the law against cyber crimes on e-wallets and how to legally protect the security of user data in the threat of data theft. The goal is to know the legal protection of consumers from personal data security risks, fraud threats, and cybercrime in the e-wallet payment system.

METHOD

The type of research in this writing is normative legal research using literature or literature methods. Normative legal research is essentially a document study that examines and examines sources of primary legal materials in the form of written regulations such as the ITE Law, Bank Indonesia Regulations, Minister of Communication and Information Regulations, legal theory, expert opinions, as well as secondary legal materials in the form of publications about e-wallet security. The law includes research results from journals, articles and other types of writing that directly relate to the problems in this research.[10]The data analysis used in this research is a qualitative data analysis technique, which is a method of data analysis by exploring the meaning and understanding of a phenomenon and connecting it with theories from literature studies and legislative approaches according to their quality and truth, which are then arranged into a systematic whole. Then conclusions are drawn so that they can answer the problem formulation in this research using a deductive writing method.[11]

ANALYSIS AND DISCUSSION

Law Enforcement against Cyber Crime on E-wallets

The increasingly advanced development of both devices and their use provides positive value for people's lives, such as the presence of e-wallets. E-wallet is a program service that archives and monitors user online shopping information, such as user login data, passwords, shipping addresses, and information regarding user credit cards.[12] Having an e-wallet will undoubtedly make it easier for everyone when they want to make transactions. Technology not only offers benefits by making people's lives easier but also has the weakness of making it easier for criminals to commit crimes. As time goes by, forms of crime become more diverse. Technological developments are one of the factors that can trigger crime. Along with the development of technology, the types of crime also develop and vary. Many new crimes have emerged along with technological developments, especially internet technology. Cybercrime is a form of crime caused by technological developments. This crime has become an international concern. Cybercrime is one of the dark sides of technological progress hurts every area of modern life today.[13] Cybercrime is an illegal act using the internet, advanced technology and telecommunications.

David S. Wall says "cybercrime broadly describes crimes that occur within that space and the term has come to symbolize online insecurity and risk."[14]Cases of e-wallet user data theft can

[10]Juhnny Ibrahim Jonandi Effendi, "Legal Research Methods: Normative and Empirical," Depok : Prenandamedia Group (2018).

[11]David Tan, "Legal Research Methods: Exploring and Reviewing Methodologies in Carrying Out Legal Research," NUSANTARA: Journal of Social Sciences (2021).

[12]Surya Bodhi and David Tan, "Security of Personal Data in E-Wallet Payment Systems Against the Threat of Fraud and Phishing (CYBERCRIME)," UNES Law Review (2022).

[13]Raodia Raodia, "The Influence of Technological Developments on the Occurrence of Cybercrime," Jurisprudentie: Department of Legal Studies, Faculty of Sharia and Law (2019).

[14]Rahel Octora, P.Lindawaty S.Sewu, and Jason Arnold Sugiono, "Regulation on Electronic System Security for E-Wallet in Order to Protect Consumers from Financial Loss Due to Cyber Fraud Based on Indonesian Law," International Journal of

occur due to fraud or phishing carried out by the perpetrators. In this case, the perpetrator of the data breach can be considered to have committed a criminal act, so criminal law enforcement is required. Criminal law is part of public law. Criminal law can be defined as rules that constitute the actions of legal subjects, which stipulate rights and obligations, what individuals may or may not do, and also the punishment for such violations. In the Indonesian legal system, determining an act as a criminal offense is based on the principle of legality, where the perpetrator of an act can be subject to sanctions based on applicable written regulations. The principle of legality is clearly stated in Article 1 (1) of the Criminal Code which is currently in force. The perpetrators carry out criminal acts in such a way that the victim provides the perpetrator with an OTP, and they can easily access the victim's e-wallet account. Such actions usually start with phishing.[15]

*Phishing*is a fraudulent attempt to obtain sensitive information, such as usernames, passwords and credit card details, by impersonating a trustworthy site in electronic communications.[16]Phishing is usually carried out via e-mail or instant messaging, and often directs users to enter website details, although telephone contacts have also been used many times. Based on the Indonesian legal system, the perpetrator's actions in illegally accessing the victim's account can qualify as a violation of Article 30 paragraphs (1) and (2) "Law No. 11 of 2008 concerning Information and Electronic Transactions" (hereinafter referred to as the ITE Law), which states "Every person intentionally and without right or against the law, accesses a computer and/or electronic system belonging to another person by any means". In paragraph (2) "Every person intentionally and without right or against the law, accesses a computer and/ or Electronic System by any means for the purpose of obtaining Electronic Information and/or Electronic Documents". Furthermore, Article 46 states that people who violate Article 30 paragraph (1) or paragraph (2) will be punished with imprisonment for a maximum of 7 years and/or a fine of a maximum of IDR 700,000,000.00. Even though there are regulations and laws governing data theft, Indonesia still does not have specific regulations governing e-wallets, so it can cause conflict if related regulations are used as a legal basis when there are legal problems. Even though there are similar arrangements with e-wallets, laws and legislatures regulating e-wallets are still needed because e-wallets and e-money are different.

Legal Protection for Personal Data Security, Threats of Fraud and Phishing (Cybercrime) on E-wallets

In Article 1 (1) Minister of Communication and Information Regulation no. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, Personal data is specific individual data stored, maintained and maintained as correct and protected as confidential. Philipus M. Hadjon provides the view that legal protection is the protection of "honor and dignity" and recognition of the human rights possessed by a legal subject.[17]Providing protection to society is the goal of law is the ultimate means of controlling various changes in society so that existing changes can also help realize the development of the nation and state in a better direction. Laws can provide solutions to use and utilize science and technology as best as possible for the benefit and survival of humans. In the context of electronic transactions, law aims to protect consumers.[18]If consumers are society, then protecting consumers means also safeguard society. One form of legitimate protection for e-wallet consumers is maintining their personal data's security. Legal protection is the protection of human rights that other people

Social Science And Human Research 04, no. 09 (2021): 2272–2279.

[15]Raodia, "The Influence of Technological Developments on the Occurrence of Cybercrime."

[16]Ardi Saputra Gulo, Sahuri Lasmadi, and Khabib Nawawi, "Cyber Crime in the Form of Phishing Based on the Information and Electronic Transactions Law," PAMPAS: Journal of Criminal Law (2021).

[17]Roberto Ranto, "Judicial Review of Legal Protection for Consumers in Buying and Selling Transactions via Electronic Media," Journal of Legal Studies: Alethea (2019).

[18]Kornelius Benuf, Siti Mahmudah, And Ery Agus Priyono, "Legal Protection for the Security of Financial Technology Consumer Data in Indonesia," Legal Reflections: Journal of Legal Studies (2019).

violate, and this protection is granted to the community so that they can enjoy all the rights given to them by law. Based the concept of privacy of data about a person, "privacy of data about a person", means that the right to privacy can also relate to information about a person collected and used by other people.[19]From this concept, we know that protecting the security of personal data is a manifestation of a person's privacy, so it is very important.

Philipus M. Hadjon revealed two types of legal protection that can be provided, namely, preventive and repressive legal protection (Preventive and repressive).[20]Protection of personal data on e-wallets must be carried out by the provider when receiving and obtaining user data, then when processing, analyzing, storing and displaying user data that has been received. If there is an interest in disseminating and destroying user personal data then protection The security of the data, process must be ensured.[21]This is reinforced in Article 26 of the ITE Law which explains that personal data is a person's right. The rights referred to in this article consist of the right to data confidentiality, complaints in the context of resolving disputes related to personal data because electronic system operators do not maintain the confidentiality of personal data, and the right to access or be able to change or update their data without disturbing the personal data management system .[22]If you want to use information from electronic means and the information is related to someone's data, you must obtain permission and approval from the person concerned. A party violating this rule, can be sued for the resulting losses. Based on the contents of this article, activities such as collecting and disseminating personal data constitute a violation of a person's right to privacy because the right to privacy includes the right to decide whether to provide personal data or not. Users of electronic systems must maintain the confidentiality of personal data obtained, collected, processed and analyzed, as well as to protect personal data and documents containing such personal data from misuse, and are responsible for personal data contained within its control, data protection guarantees are regulated in Article 15 paragraph (1) of the ITE Law, which requires every electronic system operator to maintain platform security.[23]

Bank Indonesia (BI), as the supervisor of payment system activities in Indonesia, has the obligation to supervise payment transactions through predetermined policies for efficiency and security in the payment system.[24]This can be done by monitoring existing systems and at the planning stage, assessing how each provider will carry out payment system activities based on compliance with each payment system objectives, security, and efficiency. Article 20 Paragraph (2) PBI Number 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing contains provisions regarding the implementation of information system security standards so that the aim of implementing a payment system in Indonesia which is characterized by the principles of efficiency, fluidity, security and reliability can be carried out correctly.[25]After the enactment of PBI No. 20/6/PBI/2018 concerning Electronic Money, the implementation of a policy whereby parties acting as organizers must first obtain

[19]Benuf, Mahmudah, And Priyono, "Legal Protection of Financial Technology Consumer Data Security in Indonesia."

[20]Ni Nyoman Anita Candrawati, "Legal Protection for E-Money Card Holders as a Payment Means in Commercial Transactions," Udayana Master of Law Journal (2014).but not the deposit as stipulated in the Banking Law, so it is not guaranteed by Saving Guarantee Institution (LPS

[21]AA Ngurah Deddy Hendra Kesuma, I Nyoman Putu Budiartha, And Puru Ayu Sriasih Wesna, "Legal Protection for the Security of Financial Technology Consumers' Personal Data in Electronic Transactions," Journal of Legal Preferences (2021).

[22]Law Number 19 of 2016, Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (Jakarta).

[23]Ririn Aswandi, Putri Rofifah Nabilah Muchsin, And Muhammad Sultan, "Protection of Data and Personal Information Through the Indonesian Data Protection System (IDPS," LEGISTALTIF, No. 14 (2018): 63–65.technology is very supportive to develop a business.

[24]Elsa Debora Manurung, Lastuti Abu Bakar, And Tri Handayani, "Legal Certainty in Providing Electronic Wallet Services in the Payment System is Linked to the Principles of Smooth, Safe, Efficient and Reliable Based on PBI Number 20/6/PBI/2018 Concerning Electronic Money," Journal Jurisprudence (2020).

[25]Ibid.

permission from BI by fulfilling general requirements and eligibility aspects. Article 34 of the PBI states that organizers must implement security standards in information systems, and electronic money providers are required to apply the principles of anti-money laundering, prevention of terrorism financing and consumer protection to create legal certainty for users.[26]

The existence of the OJK as a custodian in the financial services sector should protect consumers from financial services business actors who are considered to be detrimental to consumers' interests. In Article 4 of Law No. 21 of 2011 concerning the Financial Services Authority explains the purpose of establishing OJK, one of the main objectives is to protect the interests of consumers and society,[27]so that consumers feel safe when using financial services. OJK, as an institution with the authority to supervise business activities in the financial services sector, must be able to protect consumers using financial services who place their funds and/or utilize the services available at financial services institutions. Therefore, OJK through "OJK Circular Letter Number 18 /SEOJK.02/2017 concerning Governance and Information Technology Risk Management in Information Technology-Based Money Lending and Borrowing Services" xplained that personal data that must be protected is user name, residence address, identity card (such as KTP, SIM, Passport, and NPWP), date of birth, user email, IP address, user telephone number, account number, birth mother's name, credit card number, digital identity (biometric), signature, educational history, employment history, bank statements, list of assets, other related data and information.[28]However, there are still many people who only receive information but need help understanding and processing it correctly, so many still study inaccurate information.

So that personal data on e-wallets can remain safe, preventive measures are needed to prevent adverse impacts and misuse of the use of technology. According to the Ministry of Communication and Information, the action to prevent cyber crime from occurring is not to provide OTP codes carelessly. The OTP code is the most crucial thing in technology security today because it is like a house key that cannot be given to just anyone. If someone receives an SMS, telephone call, email, or even chat from an official institution or e-wallet provider that asks for an OTP code, they must be wary because the fundamental institution will never ask for an OTP code. Apart from that, Kominfo also appealed to the public to always be cautions of fake or fraudulent websites and committing fraud using call forwarding. The first Kominfo recommendation is to immediately contact the call centre of the relevant electronic money or m-banking application for complaints and handling them, after that we must report them to the authorized parties such as Bank Indonesia, police, OJK and related institutions to carry out reporting and investigations. Apart from not providing random OTP codes, cybercrime can start with us by increasing our understanding of the importance of personal data security. Understanding the public about data security with reduce the cybercrime problem that occurs the public. If preventive and repressive measures have been taken but the public does not want to care and ignores them, then the problem of personal data security will never end and will continue.[29]

[26]Richo Fernando and Eny Sulistyawati Sitorus, "Legal Protection of Electronic Money Card Holders When Lost," Novum: Legal Journal (2018).

27Law no. 21 of 2011 concerning the Financial Services Authority.

[28]Benuf, Mahmudah, And Priyono, "Legal Protection of Financial Technology Consumer Data Security in Indonesia."

[29]Kominfo, "What Should You Do If You Become a Victim of Online Fraud? This is the Kominfo Solution," Kominfo. Go.Id.

CONCLUSION

Based on the results and discussion of this research, the conclusion is that technological developments, especially in e-wallets, provide convenience in transactions but also increase the risk of cyber-crime such as phishing and scams. Law enforcement against this crime is crytical. In the Indonesian legal system, illegal actions related to e-wallet account access are regulated by the ITE Law which provides strict sanctions for perpetrators. Even though rules regarding data theft already exist, more detailed special regulations are needed for e-wallets to avoid legal conflicts.

Legal protection of personal data security and cybercrime threats on e-wallets must be a priority. Existing regulations, such as the ITE Law and Minister of Communication and Information regulations, set personal data security standards that service providers must comply with. Bank Indonesia and OJK are also important in supervising and ensuring compliance with these security standards. Preventive measures, such as education about personal data security and being alert to OTP code requests, as well as repressive measures, such as reporting and law enforcement against violators, are essential.

BIBLIOGRAPHY

Aswandi, Ririn, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan. "Protection of Data and Personal Information Through the Indonesian Data Protection System (IDPS." LEGISTALTIF, no. 14 (2018): 63–65.

Benuf, Kornelius, Siti Mahmudah, and Ery Agus Priyono. "Legal Protection for Financial Technology Consumer Data Security in Indonesia." Legal Reflections: Journal of Legal Studies (2019).

Bodhi, Surya, and David Tan. "Security of Personal Data in the E-Wallet Payment System Against the Threat of Fraud and Phishing (CYBERCRIME)." UNES Law Review (2022).

Candrawati, Ni Nyoman Anita. "Legal Protection for E-Money Card Holders as a Means of Payment in Commercial Transactions." Udayana Master of Law Journal (2014).

David Tan. "Legal Research Methods: Exploring and Reviewing Methodology in Carrying Out Legal Research." NUSANTARA: Journal of Social Sciences (2021).

Devita, Vivin Dian. "Local E-Wallets Still Dominate Q2 2019-2020." IPRICE. Last modified 2020. Accessed March 12, 2024. https://iprice.co.id/trend/insights/top-e-wallet-di-indonesia-2020/.

Eri Susanti, Ni Desak Made, Ida Bagus Putra Atmadja, and AA Sagung Wiratni Darmadi. "Legal Protection for Owners of E-Money Issued by Banks in Non-Cash Transactions." Kertha Semaya: Journal of Legal Studies (2019).

Fadila, Shifa Nur, and Yudho Winarto. "There are rampant cases of hacking into DANA's digital wallet, here's DANA's response." Kontan.Co.Id. Last modified 2023. https://keuangan.kontan.co.id/news/marak-kas-pembobolan-pada-dompet-digital-dana-begini-tunjungan-dana.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. "Cyber Crime in the Form of Phishing Based on the Information and Electronic Transactions Law." PAMPAS: Journal of Criminal Law (2021).

Jonandi Effendi, Juhnny Ibrahim. "Legal Research Methods: Normative And Empirical." Depok : Prenandamedia Group (2018).

Kesuma, AA Ngurah Deddy Hendra, I Nyoman Putu Budiartha, and Puru Ayu Sriasih Wesna. "Legal Protection for the Security of Financial Technology Consumers' Personal Data in Electronic Transactions." Journal of Legal Preferences (2021).

Kominfo. "What Should You Do If You Become a Victim of Online Fraud? This is the Communication and Information Solution." Kominfo.Go.Id.

Malia, Indiana. "Aura Kasih's balance lost IDR 11 million, important! Check BI Rules Regarding E-Wallets." IDN Times. Last modified 2019. Accessed March 24, 2024. https://www.idntimes.com/business/economy/indianamalia/saldo-aura-kasih-raib-rp11-juta-cepat-cek-aturan-bi-soal-e- wallets.

Manurung, Elsa Debora, Lastuti Abu Bakar, and Tri Handayani. "Legal Certainty in Providing Electronic Wallet Services in the Payment System is Linked to the Principles of Smooth, Safe, Efficient and Reliable Based on PBI Number 20/6/PBI/2018 Concerning Electronic Money." Journal of Jurisprudence (2020).

Michell, Cecilia, Charys Naomi Winarto, Liliyanti Bestari, Dimas Ramdhan, and Andry Chowanda. "Systematic Literature Review of E-Wallet: The Technology and Its Regulations in Indonesia." In 2022 International Conference on Information Technology Systems and Innovation, ICITSI 2022 - Proceedings, 2022.

Muhammad Taufik Hidayat, Qurrotul Aini, and Elvi Fetrina. "E-Wallet User Acceptance Using UTAUT 2 (Case Study)." National Journal of Electrical Engineering and Information Technology (2020).

Octora, Rahel, P. Lindawaty S. Sewu, and Jason Arnold Sugiono. "Regulation on Electronic System Security for E-Wallets in Order to Protect Consumers from Financial Loss Due to Cyber Fraud Based on Indonesian Law." International Journal of Social Science And Human Research 04, no. 09 (2021): 2272–2279.

Putra, Muchammad Fahryan, and Lucky Dafira Nugroho. "Legal Protection of Electronic Wallet Users for the Loss of Electronic Money." PROHUTEK Proceedings of the National Seminar on Law and Technology (2020).

Ranto, Roberto. "Judicial Review of Legal Protection for Consumers in Buying and Selling Transactions via Electronic Media." Journal of Legal Studies: ALETHEA (2019).

Raodia, Raodia. "The Influence of Technological Developments on the Occurrence of Cybercrime." Jurisprudentie: Department of Legal Studies, Faculty of Sharia and Law (2019).

Roland Fran Vernando, Diana Frederica, Christy Theodora, Victor Saputera Harefa, Sherly Sherly, and Cynthia Theodora. "Level of Effectiveness of Regulations and Security Systems in Reducing E-Wallet User Anxiety." Buana Accounting Journal (2022).

Sitorus, Richo Fernando and Eny Sulistyawati. "Legal Protection for Electronic Money Card Holders When Lost." Novum : Law Journal (2018).

Law Number 19 of 2016. Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Jakarta, nd