Jurnal Daulat Hukum
Volume 8 No.1, March 2025
ISSN: 2614-560X
SINTA 3 Decree No. 0547/ES/DT.05.00/2024
Dated May 15, 2024

Law Enforcement Against Bank Account Breach by Hackers in Perspective of Legal Law

Donius Ndruru[1)], July Esther [2)] & Debora[3)]
[1)] Faculty of Law, Universitas HKBP Nommensen, Medan, Indonesia, E-mail: donius.ndruru@student.uhn.ac.id
[2)] Faculty of Law, Universitas HKBP Nommensen, Medan, Indonesia, E-mail: julyesther@uhn.ac.id
[3)] Faculty of Law, Universitas HKBP Nommensen, Medan, Indonesia, E-mail: debora@uhn.ac.id

Abstract. *The development of information and communication technology has changed the landscape of the financial industry, particularly in digital banking. Despite offering convenience to customers through services such as internet banking and mobile banking, the risk of cybercrime, such as account breaches, is increasing. This research aims to analyse law enforcement against hackers in cases of bank account break-ins in Indonesia. The method used is a normative legal approach, which involves the study of library materials through a statutory and case approach. Data sources include primary, secondary, and tertiary legal materials, which are analysed descriptively to understand relevant legal norms and doctrines. This research found that despite the existence of various laws related to personal data protection and cybercrime, challenges in law enforcement remain, including a lack of public awareness and adequate human resources. In recent years, bank account breaches have become more prevalent, with various modes that are increasingly sophisticated and difficult to detect. Real-life cases, such as the arrest of 35-year-old Palembang-born porters and hacker syndicate member Gerri Harri Wijaya, serve as important examples in highlighting the need to improve customer protection and banking system security. To stop similar atrocities, more public education and awareness is needed. The results of this study are expected to provide insights for the government, law enforcement agencies, and the banking sector in creating a safe environment for digital financial transactions, as well as raising public awareness about the risks of cybercrime.*

Keywords: *Bank; Cyber; Hackers; Security.*

1. Introduction

The development of information and communication technology has a profound effect on many aspects of life, including the financial industry. Banks, as financial institutions that ensure customer security and trust, are now facing new challenges due to the rise of cybercrime, especially the breach of bank accounts by hackers. These incidents not only harm banks, but also cause significant losses to customers who lose their funds and personal data.

This can be evidenced by the widespread use of the term "digital banking" in the banking industry. Digital banking is a banking service that utilizes applications and technology to align with the evolution of the growing digital economy. With the widespread use of digital banking services, such as internet banking and mobile banking, it is important to understand the risks that come with it (Dewi et al., 2023).

The emergence of increasingly sophisticated modes of crime in bank account break-ins raises serious questions about the effectiveness of existing law enforcement. Cases such as the one involving Gerri Harri Wijaya show that while perpetrators may not have high hacking skills, creative fraud methods can result in substantial losses for victims. Gerri's modus operandi was to send a marriage invitation application via WhatsApp, which was used to defraud victims. The arrest was made by East Java Police on July 26, 2023, after the victim reported on July 5, 2023. Gerri was arrested in Palembang, and the case file was declared complete on October 18, 2023 before being transferred to the Malang prosecutor's office. This case reveals the importance of public vigilance against technology-based fraud. Therefore, it is necessary to conduct an in-depth analysis of the challenges faced in law enforcement against this cybercrime (Rahman, 2023). Based on information from Antara News presents that there are 32 total cases of bank account break-ins (Antara News, 2024).

This research is very important to do considering the high number of cybercrimes in the banking sector and its impact on public trust. This research will provide insight into how law enforcement in Indonesia can be improved to protect customers and prevent similar crimes in the future. By understanding this issue, it is hoped that better solutions can be found in improving the security of the banking system. Indonesia has enacted a policy on the protection of formally controlled personal data. The state is responsible for protecting the personal information of Indonesian individuals in light of various cases of ATM theft, bank account breaches, hacking and theft. Therefore, Law No. 27 of 2022 on Personal Data Protection (UU PDP) is a set of laws and regulations enacted or adopted by the government in 2022 (Watkat et al., 2024). By protecting personal data, the privacy of bank customers will be maintained and unauthorized parties or hackers will not be able to misuse it (Sibagariang & Parhusip, 2024).

This research offers solutions in the form of a comprehensive analysis of law enforcement measures that can be applied in cases of bank account breaches. In addition, this research will also provide policy recommendations to improve collaboration between law enforcement agencies and the banking sector, as well as increase public awareness about the risks of cybercrime. Law enforcement is a collection of procedures that interpret rather abstract values, concepts, and aspirations, namely, legal objectives. Moral principles that should be applied in reality, such as justice and truth are part of the purpose of law (Alelxander, 2023). Law enforcement agencies often rely on the provisions articulated in the Criminal Code (KUHP) (Bupu et al., 2024), despite the existence of Law No. 1 of 2024 on the second amendment to Law No. 11 of 2008 and Law No. 19 of 2016 on Electronic Information and Transactions in

cases of carding (cybercrime). This makes it easier to avoid legal problems because the law is not easily enforced.

Several previous studies have examined aspects of law enforcement in the context of cybercrime. First, research by Dewi et al. (2023) showed that many customers suffered losses due to vulnerabilities in digital banking services (Dewi et al., 2023). Second, Kamila & Rahayu (2024) emphasized the importance of strong technological infrastructure to prevent cybercrime (Kamila & Rahayu, 2024). Third, research by Rahman (2023) highlighted the need for public education on the risks of technology-based fraud. In contrast to these studies, this research not only addresses the technical and educational aspects, but also focuses on effective law enforcement as a solution to address the problem (Rahman, 2023). Although the government and relevant organizations have released a number of laws and guidelines to combat cybercrime, law enforcement continues to face a number of challenges. The problems themselves include the general public's ignorance of cybersecurity threats and the scarcity of qualified human resources to combat cybercrime.

This research aims to analyze the law enforcement that can be done to hackers in bank account break-in cases. Thus, law enforcement can provide legal certainty, expediency, and justice. Furthermore, this research aims to provide policy recommendations that can improve the protection of customer personal data and create a safer environment for digital financial transactions. By understanding the dynamics of this issue, it is hoped that this research can contribute to improving the security of the banking system in Indonesia and facilitating more effective law enforcement against cybercrime.

2. Research Methods

This research uses a type of normative legal research regarding law enforcement against bank account break-ins by hackers. This type of research examines various laws and regulations, such as the 1945 Constitution of the Republic of Indonesia, the Criminal Code, Law Number 10 of 1998 concerning amendments to Law Number 7 of 1992 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 and Law Number 19 of 2016 concerning Electronic Information and Transactions. Nanang Martono formulated that research is a process to find answers to a particular problem, then using scientific methods; a collection of methods used in a systematic way will find answers to problems to produce knowledge insights (Solikin, 2019). The object of this research leads to law enforcement that can be done to hackers in cases of breaking into bank accounts.

The method used in this research is a normative legal research approach. The normative legal research approach is a library research method by examining library materials that are relevant to the object of study. This research uses a statute approach, and a case approach. The method taken in this research is to use objects in the form of legal norms to answer the legal problems faced through the process of finding legal rules, legal principles, and legal

doctrines. The source of research legal material is document and literature studies, legal research conducted by examining various library materials. With a research focus on document and literature studies, the legal materials used in this research can be primary legal materials, secondary legal materials, and tertiary legal materials. Legal materials are used to examine existing problems.

The data sources used in this research include: First, primary legal materials are legal sources that have binding force and are the basis of the legal system. This material examines various laws and regulations issued by authorized institutions. Second, secondary legal materials are legal sources that provide explanations, interpretations, or opinions on primary legal materials. Although it does not have binding force, this material is very important in understanding and applying the law. This research uses secondary legal materials by reviewing various literature, namely: books, journals, theses, theses, and the internet. Third, tertiary legal materials are sources that assist in finding and understanding other legal materials, but do not directly regulate the law. This material is usually informative and helps in finding primary legal materials and secondary legal materials. This research uses tertiary legal material, namely dictionaries. To draw conclusions, this research uses descriptive data analysis, which involves retrieving factual data, summarizing, and characterizing findings from the literature by combining relevant laws and regulations with various literature in the form of books, journals, theses, theses, and the internet related to the research problem. By using a normative legal research approach, data analysis in this study looks at various materials related to law enforcement that can be applied to hackers in the event of a bank account break-in.

3. Results and Discussion

3.1. Law Enforcement that can be done to Hackers in Bank Account Breach Cases

Banks are an integral element of the financial system and payment system in a country (Chotidjah et al., 2022), in the current era of globalization banks also play a role in the international financial and payment system. After obtaining a license to operate from the monetary authority locally, the bank belongs to the community. As a financial institution, banks rely heavily on the full trust of customers who entrust their funds and use the services offered. Therefore, banks have a great interest in maintaining a high level of trust from the public, both those who have and will deposit money in the bank, as well as those who have or will utilize other services. Law Number 10 of 1998 Article 1 Paragraph (2) on Banking reads:

> *"Bank is a business entity that collects funds from the public in the form of deposits and distributes them to the public in the form of credit and or other forms in order to improve the lives of many people".*

Banking functions as an institution that has an important role in the development of a country. The role of banking is very functional in financial intermediary institutions, namely collecting

funds from the public in the form of deposits and channeling them in the form of credit or other forms to improve the welfare of the community. Every activity carried out by banks is always related to various commodities, such as moving money, receiving and paying money from accounts, discounting bills of exchange, and buying and selling , checks, bills of exchange, and trade papers, including buying collateral (Chotidjah et al., 2022).

Today's society is always fast moving towards modernization and this also applies to the law. Law and society are interconnected and must develop simultaneously for the law to remain effective in regulating life. Technological advancements in society can affect the types of crimes that emerge, including the rise of cybercrime. The increased use of the internet in Indonesia has led to a significant spike in cybercrime cases including cases of bank account breaches committed by by hackers. Cybercrime has now penetrated the banking sector, where banking security systems continue to face challenges from high-tech breaches and abuses that affect their operations. Cybercrime utilizes information technology to commit illegal acts, which is one of the negative impacts of the rapid development of the internet and technology (Idris Balaka et al., 2024).

According to Muhammad Djumhana (Djumhana, 2003), banking law is a set of laws that regulate the operation of banking and financial organizations with various aspects, essence, and existence, as well as their relationship in other areas of life. Banking includes all things related to banks, including institutions, business operations, and the process of implementing these operations. According to Munir Fuadi (Fuadi, 1999), banking law is the body of laws that regulate banking affairs. It is a body of legal guidelines consisting of Acts, regulations, jurisprudence, doctrine, and other sources of law that govern banking as an organization, the details of its day-to-day operations, the requirements that banks must meet, the conduct of its officials, the rights, duties, and responsibilities of the parties involved in the banking industry, the existence of banking, and other matters relating to the banking industry. The main role of banking as an intermediary is to collect public funds and distribute them effectively or efficiently through the real sector, which encourages the growth and economic progress of a country (Idris Balaka et al., 2024). The customer's relationship with the bank becomes the level of trust in collecting and storing money or funds in the bank and the bank's protection of customers or the public in preventing account breaches committed by hackers.

Banking institutions in Indonesia rely heavily on the principle of trust upheld by the public for operational continuity. Therefore, to maintain public trust, the government plays an active role in protecting bank customers. If there is a significant decline in the level of public trust in banking institutions, this can have a serious impact on the country's economy and is difficult to repair. Legal protection for customers is crucial. One of the bank's responsibilities is to ensure the security of customers' personal data, which includes information that can be used to identify individuals (Bhoki et al., 2024). Legal protection is an important element in a state of law, because it serves to protect individuals who feel harmed, thus creating a sense of security and comfort. Everyone realizes that banks have a crucial role in the banking sector, and legal protection for customers is necessary in the event of a loss. With this protection, customers

can claim compensation or other appropriate measures. This form of protection is essentially an effort to ensure safety, which requires a conceptual understanding to harmonize the various rules in legal protection in the banking world (R. T. Putra et al., 2020).

On Monday, October 17, 2022, President Joko Widodo signed Law Number 27 of 2022 on Personal Data Protection (PDP Law). The PDP Law Policy is an implementation of Article 28G, Paragraph 1 of the 1945 Constitution of the Republic of Indonesia, which reads:

> *"Every person shall have the right to the protection of his or her person, family, honor, dignity, and property under his or her control, and shall have the right to security and protection from threats of fear to do or not to do something which is a human right".*

It is hoped that this Act will provide a strong legal basis for the administration and safeguarding of personal information of the public and government officials. The 16 chapters and 76 articles that make up the Personal Data Protection Law (PDP) regulate a number of topics, including the transfer of personal data, administrative sanctions, institutions, international cooperation, public participation, dispute resolution, procedural law, prohibitions on the use of personal data, criminal provisions, and provisions for rescue and closure. The universal and globally recognized Article 28G of the 1945 Constitution also mentions the protection of personal data. Meanwhile, the government is working to provide legal clarity to the banking industry with Law Number 10 of 1998, which updates Law Number 7 of 1992 governing Banking. The principles, role, and purpose of banks, the requirements that banks must meet, the conduct of bank officers, and the rights, duties, responsibilities, and obligations of banks are just some of the topics covered in the Act. Actors and related parties in the financial sector are also governed by these regulations. Provisions relating to bank secrecy, defined in Article 1 Paragraph (28) as any information relating to customers and their deposits, protect the privacy rights of consumers. Regulations relating to violations of breaches of bank secrecy are set out in Article 47 Paragraphs (1) and (2), in order to enhance the protection of customers' personal data (Jonimandala et al., 2023).

The rights of the customers involved are violated when someone breaks into a bank account. Not everyone can break into a bank account because this kind of crime falls under the category of white collar crime, which requires the commission of a crime. high level of intelligence and technology (Aini & Khoiroh, 2024). For many internet users, cybercrime is a very bad thing (Indah et al., 2022). Bank account thieves usually have a thorough understanding of the banking industry's transaction procedures and utilize cutting-edge computer technology (Maymuna, 2024). Law Number 10 of 1998 on Banking, which regulates the legal protection and responsibility of banks to stop hackers from breaking into bank accounts. Law Number 10 of 1998 Article 29 Banking reads:

a) *The guidance and supervision of banks is conducted by Bank Indonesia.*

b) *Banks are required to maintain a sound level of bank health in accordance with the provisions of capital adequacy, asset quality, management quality, liquidity, profitability, solvency, and other aspects related to the bank's business, and must conduct business activities in accordance with prudential principles.*

c) *In providing credit or financing based on Sharia Principles and conducting other business activities, banks are required to adopt methods that are not detrimental to the bank and the interests of customers who entrust their funds to the.*

d) *For the benefit of customers, banks are obliged to provide information regarding the possibility of the risk of loss in connection with customer transactions conducted through the bank.*

e) *The provisions that must be fulfilled by banks as referred to in paragraph (2), paragraph (3), and paragraph (4) shall be stipulated by Bank Indonesia.*

A hacker is a person who studies, analyzes, breaks into, and modifies computer systems and networks, either for personal gain or out of a sense of challenge. The term "hacker" in English originally appeared with a positive connotation, referring to someone with computer skills who could create programs in a more sophisticated or better way than the ones that were used (Cahyadi, et al., 2024). Hackers are people who can find weaknesses in a system or network and use them to access the system without authorization (Sucia, et al., 2022). Hackers are always coming up with new strategies and tactics, and they often use cutting-edge methods to avoid discovery (J. S. A. A. M. Putra, 2023). Hackers do what they do because Terrorist Groups are organizations that commit acts of terrorism, Organized Crime are organizations that commit crimes, Nattion-States are organizations that conduct intelligence operations, and Tbrill Seekers are individuals who seek self-indulgence (Kurniawan & Maujuhan Syah, 2022). A break-in can be understood as the act, procedure, and process of breaking in, according to the online Indonesian Dictionary (KBBI). "Breaking into" refers to breaking or destroying, breaking and causing damage, or dismantling by force. One of the cybercrimes committed by hackers is bank account breach, which involves entering a customer's bank account without the consent of the customer or another person.

The law enforcement process seeks to achieve three legal objectives: justice, utility, and legal clarity. According to Satjipto Rahardjo (Utama, et al., 2021), law enforcement is an effort to carry out the objectives of legislation expressed in regulations. However, the implementation of the Law does not always go according to plan. The law enforcement process is influenced by several things. Lawrence M. Friedman (Utama, et al., 2021) asserts that the three elements of legal structure, legal substance, and legal culture have an impact on how successful law enforcement is. Law enforcement officers who carry out The process of law enforcement is referred to as the legal structure, the applicable regulations are referred to as the substance of law, and the norms accepted by certain groups and obeyed by the community are referred to as legal culture. Legal development continues to evolve over time in response to the needs of

society and the government's objectives to implement legal development, rather than being limited to the three elements of the legal system. Law enforcement, or the application of current laws by law enforcement officers and organizations, is another component factor. It also includes initiatives to guarantee legal communication and information when implementing legal developments in the digital age (Warneri, et al., 2023). One of the difficulties for the law enforcement process is to determine the location and tempus delicti in the prosecution of cybercrime. The location of the crime is known as locus delicti, and the time of the crime is known as tempus delicti (B, et al., 2024).

In Indonesia, law enforcement officials authorized to handle cases of bank account breaches committed by hackers are divided into three categories:

1. Police

   The police is a law enforcement agency entrusted with enforcing the law, safeguarding and rescuing the population, and offering community services. Law Number 2 of 2002 governing the Indonesian National Police regulates the responsibilities of the police. According to Article 14 of Law Number 2 of 2002 concerning the Indonesian National Police, one of the duties of the police is to carry out government functions in order to provide protection, foster peace, maintain society, and enforce the law. The law enforcement process carried out against hackers in cases of bank account break-ins by the police includes: First, bank customers report the case account breach to the police. Second, the police collect evidence and conduct an investigation. Third, the police arrest the suspected hacker. Fourth, the suspect is imprisoned for investigation purposes. Fifth, the police make a report on the results of the investigation or make an Investigation Report (BAP).

2. Attorney

   The government agency that exercises state authority in the field of inheritance under the Act is the Public Prosecution Service, also known as the Public Prosecution Service. As a non-ministerial organization, the AGO is independent of any ministry. It reports directly to the President and is headed by the Attorney General. The AGOs that are organized into various jurisdictions throughout Indonesia, from provincial to district level are led by Ministers whose duties are equivalent to those of the Attorney General. In the Indonesian criminal justice system, the Attorney General's Office functions as a legal defense. The law enforcement process carried out against hackers in bank account break-in cases by the AGO includes: First, the prosecutor's office receives a BAP from the police after the police make a report on the results of the investigation. Second, the prosecutor's office files an indictment against the suspect. Third, the prosecutor's office collects additional evidence if needed. Fourth, the prosecutor's office prepares the case to be submitted to court or tried.

3. Court

Any case filed by the public must be heard, decided, and resolved by the court, which is an official government entity. If all parties are present to participate, the court settlement process can proceed. Judges and disputing parties are expected to follow the rules honestly and in accordance with the relevant laws. The litigants want the lawsuit They are resolved fairly and in a way that meets their expectations (Hidayatullah et al., 2023). The law enforcement process carried out against hackers in cases of bank account break-ins by the courts includes: First, the judge reads out the charges against the suspect. Second, the prosecutor reads out the charges. Third, the suspect or his lawyer defends himself or the suspect's defense. Fourth, the judge decides on the verdict and sentence. Fifth, the judge reads out the final decision on the results of the judges' decisions. As stated in Article 184 of the Criminal Procedure Code (KUHAP), valid evidence is needed to support the proof of the crime of bank account break-in by hackers in the trial. This includes witness statements, expert testimony, letters, clues, and defendant statements.

Law enforcement often faces challenges in carrying out its functions due to the dynamic and diverse conditions of society, as well as a legal system that requires the application of positive legal rules (Esther et al., 2020). Law enforcement must take action against violations that occur. Law enforcement relies heavily on legal certainty as protection against capricious behavior. People seek legal clarity because it fosters peace, security and harmony. Bank customers also expect law enforcement to provide tangible benefits because the law is intended to protect society, so its implementation must provide and advantages to society. A peaceful and healthy environment will be realized when people get good services. Law plays a role in protecting the rights and obligations of every individual, and strong legal protection aims to create peace, security, tranquility, welfare, truth and justice. The basis of the Indonesian criminal justice system is the resolution of criminal cases by punishing the perpetrators. Based on evidence Criminal charges are a threat to any criminal behavior, whether it falls under the Criminal Code or not. Indonesia respects the principles of national sovereignty as the law of the state of law enforcement which must be applied in a fair, honest, and orderly manner in accordance with the Criminal Procedure Law (Ndruru & Esther, 2024). The formal and material criminal law is not adequately supported by Indonesian laws and regulations governing cybercrime. some initiatives to control rules and regulations that can stop the unfavorable effects of legal action (Oktaviani & Rusdiana, 2023). In criminal law, punishment has the dual purpose of educating and improving offenders in addition to frightening or threatening them (Sariani, 2024).

The police have taken a number of measures to address the crime of bank account break-ins, including posting appeals on social media and other platforms. The police also disseminate information to the public through newspapers, radio, and through talk shows. The police are committed to taking every case of bank account breach seriously. The police cooperate with various relevant agencies to apprehend criminals, based on public reports and make arrests at

the scene. Suspects are escorted to the police station for additional processing after arrest, and then they are handed over to the prosecutor's office. After being handed over to the prosecutor, the prosecutor's office processes them and proceeds to court for trial (Farsyak, 2024).

There are three ways to deal with bank account break-ins, namely preventive, repressive, and curative: a) Preventive measures are efforts to stop bank accounts from being breached. There are three ways to think about criminal policy: narrow, broad, and very broad. Criminal policy, in its strictest definition, refers to the principles and strategies that serve as the basis for actions taken in response to violations of the Criminal Code. This policy, in its broadest sense, encompasses all aspects of law enforcement, including the protocols to which the police and government adhere. Criminal policy, on the other hand, in its broadest sense, includes all actions taken to enforce fundamental social standards through laws, rules and official institutions. One way to understand the enforcement of these standards is as an attempt to deal with criminality. It is not just the police who are responsible for preventing bank account breaches. Moreover, there are other techniques to avoid crime in general that may not normally fall under the criminal justice system. Social assistance, for example, can serve as a diversion for young people from criminal activity (Susandi, 2024). b) Repressive measures are any actions taken by law enforcement after a bank account breach are considered repressive. Investigation, prosecution, and imposition of criminal fines are examples of repressive activities. All of these activities fall under the category of criminal policy and should be viewed as a series of steps taken by the appropriate authorities to deal with crime. c) Curative measures are broad-based preventive measures to address bank account breaches. Curative measures, which target criminals more specifically, are seen as the antithesis of oppressive measures. Officer Criminal execution, such as officers from Community Guidance and Child Removal (BISPA) or prison officers, are immediately responsible for these actions. Regardless of the success or failure of the process, they are involved in coaching (Susandi, 2024).

There is now a lack of stringent security measures against cybercrime, and hackers using various techniques continue to break into bank accounts. Theft in the contemporary criminal world includes not only the unlawful taking of tangible objects but also the unlawful taking of personal information. Many hackers are directly or indirectly responsible for the theft of commercial and personal data, especially financial data stored on computers or the internet. Because bank account theft is so complex and raises a host of new issues both domestically and internationally, law enforcement must act quickly to protect bank customer data (Arumawan, 2023). the country where the perpetrator is located to allow them to be arrested is one way countries with jurisdiction over criminals in other countries can take action (Singgi et al., 2020).

According to Articles 30 and 32 of Law Number 1 Year 2024 on Electronic Information and Transactions, hackers who break into bank accounts by misusing various digital banking services without the consent of the owner or another person can be punished. These articles contain provisions relating to the admissibility of electronic information as evidence in court as

well as prohibitions on crimes that harm the parties involved, such as data theft. The confidentiality of consumer bank accounts and offenses that cause harm to customers, such as theft of bank accounts, are regulated by Law Number 10. Year 1998 on Banking. The Criminal Code Article regulates theft as one of its operational modes, and Law No. 27 of 2022 on Personal Data security, which regulates the security of customers' personal data to prevent bank account breaches (Arumawan, 2023). Article 362 of the Criminal Code reads:

> *"Any person who takes property, wholly or partially belonging to another, with intent to unlawfully possess it, shall, being guilty of theft, be punished by a maximum imprisonment of five years or a maximum fine of six hundred Rupiahs".*

4. Conclusion

This research emphasizes the importance of law enforcement against hackers who break into bank accounts, with the main objective of protecting public funds and maintaining customer confidence in banking institutions. The novelty of this research lies in the in-depth analysis of the collaboration between law enforcement agencies including the police, prosecutors, and courts in dealing with increasingly complex cyber crimes. This research suggests the need for a comprehensive approach that includes preventive, repressive, and curative measures to effectively address cybercrime. In addition, emphasis on the importance of training and capacity building of human resources in relevant agencies is a key factor in dealing with this challenge. By strengthening the legal framework and improving the professionalism of law enforcement officers, it is hoped that the justice system can function more effectively in protecting customers and preventing future crimes. Recommendations for future research also include evaluating the effectiveness of inter-agency collaboration in handling cybercrime, which is expected to contribute significantly to the security of the banking system in Indonesia.

5. References

Books & Journals:

Aini, A. Q., & Khoiroh, E. F. (2024). Perlindungan Hukum Nasabah dalam Kasus Pembobolan Rekening Bank di Indonesia. *Jurnal Multidisplin Ilmu Akademik*, *1*(6), 168.

Alelxander, A. (2023). Peran Masyarakat dalam Penegakan Hukum di Indonesia. *IJOLARES : Indonesian Journal of Law Research*, *1*(1), 12.

Arumawan, D. P. (2023). *Upaya Kepolisian dalam rangka menjaga Keamanan Sistem M-Banking terhadap ancaman serangan siber melalui Teknik Scamming*. Skripsi, Universitas Lampung.

B, et al., H. (2024). Peran Locus dan Tempus Delicti dalam Menentukan Kompetensi Pengadilan pada Kasus Kejahatan Siber. *Julia: Jurnal Litigasi Amsir*, *11*(3), 391.

Bhoki, A., Aloysius, S., & Bire, C. M. D. (2024). Perlindungan Hukum Terhadap Kebocoran Data Nasabah Ditinjau dari Undang-undang Nomor 10 Tahun 1998 tentang Perbankan. *Petitum Law Journal*, *2*(1), 252.

Bupu, A. G., Medan, K. K., & Amalo, H. (2024). Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu. *Jurnal Ilmu Hukum Dan Sosial*, *2*(2), 368.

Cahyadi, et al., B. (2024). Hacker Anak Dalam Perspektif Teori Differential Association: Studi Kasus Peretasan Situs Pengadilan Negeri Kabupaten Konawe. *IKRA-ITH HUMANIORA : Jurnal Sosial Dan Humaniora*, *8*(1), 333.

Chotidjah, et al., Erna. (2022). *Pengantar Hukum Perbankan di Indonesia.*

Dewi, D., Desthabu, M., & Angelica, Z. (2023). Perlindungan Hukum Nasabah BTPN Jenius Dalam Kasus Pembobolan Dana Rekening. *Fairness and Justice: Jurnal Ilmiah Ilmu Hukum*, *21*(1), 9.

Djumhana, M. (2003). *Hukum perbankan di Indonesia.* Bandung: PT Citra Aditya Bakti.

Esther, J., Naibaho, B. M., & Christine, B. (2020). Mediasi Penal Dalam Penanganan Pelaku Tindak Pidana Sebagai Upaya Meminimalisir Kelebihan Hunian Di Lembaga Pemasyarakatan. *Nommensen Journal of Legal Opinion*, *1*(1), 28.

Farsyak, V. (2024). Peran Penegak Hukum dalam Menangulangi Kejahatan Siber di Era Digital. *Jurnal Hukum Dan Kewarganegaraan*, *6*(7), 7.

Fuadi, M. (1999). *Hukum perbankan modern berdasarkan Undang-Undang tahun 1998* (Buku kesatu). Bandung: PT Citra Aditya Bakti.

Hidayatullah, T. A., Ismansyah, & Mulyati, N. (2023). Perlindungan Hukum terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan dengan Pencurian Data. *Unes Law Review*, *6*(1), 1360.

https://www.antaranews.com/tag/pembobolan-rekening-bank/2 accessed on Tuesday, 17 December 2024, at 13.31 WIB.

Idris Balaka, K., Rahman Hakim, A., & Dwi Sulistyany, F. (2024). Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital. *Yustitiabelen*, *10*(2), 112.

Indah, F., Sidabutar, A., & Annisa, N. (2022). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 3.

Jonimandala, G. W., K.G.Sondakh, D., & Sondakh, J. (2023). Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskrim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian dan Penyalahgunaan Data Pribadi. *Journal Of Social Science Research*, *3*(4), 693.

Kamila, T. P., & Rahayu, Y. S. (2024). Pengaruh Keamanan, Kepercayaan, dan Risiko Terhadap Penggunaan Layanan Mobile Banking Pada Mahasiswa di Kota Malang. *An-Nisbah: Jurnal Perbankan Syariah*, *5*(1), 49.

Kurniawan, D., & Maujuhan Syah, A. (2022). The Impact of Bjorka Hacker on the Psychology of the Indonesian Society and Government in a Psychological Perspective. *CONSEILS: Jurnal Bimbingan Dan Konseling Islam*, *2*(2), 55.

Maymuna, N. F. (2024). *Perlindungan Hukum terhadap Nasabah atas Pembobolan Rekening melalui Mobile Banking di Indonesia*. Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim.

Ndruru, D., & Esther, J. (2024). Perspektif Hukum Pidana Terhadap Tindak Pidana Penipuan Oleh Oknum Tentara Nasional Indonesia Berdasarkan Keadilan Restoratif. *Law, Development & Justice Review*, *7*(2), 159.

Oktaviani, A., & Rusdiana, E. (2023). Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi Dan Transaksi Elektronik. *Novum: Jurnal Hukum*, *10*(1), 250.

Putra, J. S. A. A. M. (2023). Hacking As A Challenge For Change And The Development Of Cyber Law In Indonesia. *Jurnal Ilmu Hukum Tambun Bungai*, *8*(2), 345.

Putra, R. T., Budiartha, I. N. P., & Ujianti, N. M. P. (2020). Bentuk Perlindungan Hukum bagi Nasabah terhadap Pembobolan Rekening Nasabah oleh Pegawai Bank. *Jurnal Interpretasi Hukum*, *1*(2), 183.

Rahman, P. F. (2023). *Polisi Limpahkan Kasus Hacker Bobol Rp 1,4 Miliar Ke Kejari Malang*. Detikjatim. https://www.detik.com/jatim/hukum-dan-kriminal/d-6989987/polisi-limpahkan-kasus-hacker-bobol-rp-1-4-miliar-ke-kejari-malang.

Sariani, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil: Jurnal Ilmu Sosial, Politik, Dan Hukum*, *2*(2), 72.

Sibagariang, D. N., & Parhusip, N. A. (2024). Peran dan Efektivitas Undang-Undang Perbankan dalam memberikan Perlindungan Hukum bagi Korban Pembobolan Rekening di Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, *1*(6), 78.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 336.

Solikin, H. N. (2019). *Pengantar Metodologi Penelitian Hukum*.

Sucia, et al., F. (2022). Pertanggungjawaban Pidana Terhadap Pelaku Hacker Dengan Tujuan Pemesanan Fiktif. *Jurnal Dialektika Hukum*, *4*(2), 158.

Susandi, P. F. (2024). *Upaya Kepolisian dalam menanggulangi terjadinya Cyber Hacking dalam Modus Pembobolan M-Banking*. Skripsi, Universitas Lampung.

Warneri, et al., M. R. (2023). *Indeks Pembangunan Hukum di Indonesia Tahun 2021*.

Watkat, F. X., Ingratubun, M. T., & Apriyanti, A. (2024). Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana Di Indonesia. *Jurnal Hukum Ius Publicum*, *5*(1), 155.

Regulation:

The 1945 Constitution of the Republic of Indonesia.

Criminal Law (KUHP).

Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 and Law Number 19 of 2016 concerning Electronic Information and Transactions.

Law Number 10 of 1998 concerning amendments to Law Number 7 of 1992 concerning Banking.

Law Number 27 of 2022 concerning Personal Data Protection.