International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 11, Issue 12
December, 2024
Pages: 231-238

The Strategy of the Financial Services Authority in Addressing the Evolution of Banking Crimes

Dwi Rimadona[1]; Enny Mirfa[1]; Dita Febrianto[2]; Siti Nurhasanah[2]; Kasmawati[2]

[1] Universitas Samudra, Indonesia

[2] Universitas Lampung, Indonesia

http://dx.doi.org/10.18415/ijmmu.v11i12.6395

Abstract

This study discusses the strategies implemented by the Financial Services Authority (OJK) in addressing the evolution of banking crimes in the digital era. Along with the rapid development of digital technology, the banking sector faces new, increasingly sophisticated threats such as cybercrime, online fraud, and personal data theft. In facing these challenges, OJK formulates policies and regulations that prioritize customer protection, strengthening digital security systems, and enhancing inter-agency collaboration. This study also evaluates the preventive and reactive measures taken by OJK, including the implementation of advanced security technologies and public education on banking crimes. Finally, the study provides recommendations on the importance of international collaboration and adaptive regulatory updates to address the continuously evolving threats.

Keywords: *Financial Services Authority; Banking Crimes; Digital Security Regulation*

Introduction

The background regarding the strategies of the Financial Services Authority (OJK) in facing the evolution of banking crimes is closely related to the rapid development of information technology and digitalization, which has had a significant impact on the banking sector. As technology advances, the methods and modus operandi of banking crimes have also become more sophisticated and diverse, taking advantage of the vulnerabilities in an increasingly connected and digital financial system.[1] Banking crimes, which were previously more conventional, such as physical theft or fraud in banks, have now evolved into digital threats that are more difficult to detect and address. These criminal modes not only threaten the banking sector but also harm customers and disrupt the overall stability of the financial system.[2]

[1] Anggoro, S. B., Amrullah, A., Tanuwijaya, F., & Anggono, B. D. (2024). Perbandingan Sistem Penegakan Hukum Kejahatan Perbankan di Era Digital di Negara Maju Dan Berkembang. *Syntax Literate; Jurnal Ilmiah Indonesia*, *9*(10), 5381-5391.

[2] Aprita, S. (2021). Kewenangan Otoritas Jasa Keuangan (OJK) Melakukan Penyidikan: Analisis Pasal 9 Huruf C Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan. *Jurnal Ilmiah Universitas Batanghari Jambi*, *21*(2), 550-563.

One of the increasingly prevalent types of crime is cybercrime, which involves the use of technology to hack into banking systems or launch cyber-attacks. These crimes include various forms of digital fraud, such as phishing, where criminals attempt to obtain sensitive customer information like credit card numbers, passwords, and PINs via fake emails or websites. There is also malware, which is inserted into customers' devices to steal personal data and access bank accounts.[3] Another emerging threat is ransomware, where criminals infect bank or customer computer systems with malicious software and then demand a ransom to restore access to locked data. Furthermore, skimming, the theft of credit or debit card data using specialized tools attached to ATMs or payment devices, remains a significant issue in the banking sector.[4]

Online fraud is also an increasingly common modus of banking crime. Perpetrators use psychological manipulation techniques to convince victims to transfer money or provide sensitive personal information. In some cases, criminals impersonate bank officers or government officials to make the victim feel secure and more likely to fall for the scam. In other forms, criminals may engage in investment scams, where they offer fake investments with promises of high returns to attract funds from customers.

Additionally, identity theft has become a more alarming modus operandi, where criminals obtain customers' personal data, such as names, addresses, identification numbers, and account information, through insecure devices or cyber-attacks on financial institutions. This stolen data is then used to make illegal transactions or is sold on the black market.[5]

In light of these various crime modes, OJK faces significant challenges in creating a system capable of countering these threats. OJK must take both preventive and reactive measures to address the ongoing evolution of banking crimes.[6] One of the strategies implemented by OJK is strengthening digital security regulations in the banking sector. In this regard, OJK encourages banks and financial institutions to adopt state-of-the-art security technologies, such as two-factor authentication (2FA) and data encryption to protect customer information. OJK also collaborates with relevant parties to develop personal data protection regulations, recognizing the importance of safeguarding customer data from theft or misuse.[7]

In addition to regulations, OJK also promotes financial literacy and education for the public. The educational programs carried out by OJK aim to increase customer understanding of how to protect their personal data, recognize signs of fraud, and avoid risks posed by banking crimes.[8] One form of education involves spreading information related to digital awareness and the importance of using secure payment systems. These educational programs are not only targeted at customers but also at all financial industry players to ensure they have a good understanding of transaction security and data management.

Moreover, OJK strengthens collaboration between institutions, both at the national and international levels, to combat banking crimes. This is done by sharing information about emerging crime modes and creating mechanisms that allow for more effective and timely responses to banking crimes. In

[3] Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *2*(1), 01-16.

[4] Cholik, C. A. (2021). Perkembangan teknologi informasi komunikasi/ICT dalam berbagai bidang. *Jurnal Fakultas Teknik UNISA Kuningan*, *2*(2), 39-46.

[5] Diba, N. F., Disemadi, H. S., & Prananingtyas, P. (2020). Kebijakan Tata Kelola Otoritas Jasa Keuangan (OJK) Di Indonesia. *Ekspose: Jurnal Penelitian Hukum dan Pendidikan*, *18*(2), 868-876.

[6] Fachrurrazy, M., & Siliwadi, D. N. (2020). Regulasi Dan Pengawasan Fintech Di Indonesia: Persfektif Hukum Ekonomi Syariah. *Al-Syakhshiyyah Jurnal Hukum Keluarga Islam dan Kemanusiaan*, *2*(2), 154-171.

[7] Ekayani, L., Djanggih, H., & Suong, M. A. A. (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan. *Journal of Lex Philosophy (JLP)*, *4*(1), 22-40.

[8] Fadlan, A. F. (2022). *Bank dan lembaga keuangan lainnya*. Publica Indonesia Utama.

this regard, OJK participates in collaborations with Bank Indonesia, the police, and international organizations such as Interpol to increase awareness of cross-border crime threats.

Overall, OJK strives to face the evolution of banking crimes with a more comprehensive approach, including strict regulations, improved public literacy, and collaboration between various parties to create a safer and more transparent financial ecosystem. Through these efforts, OJK hopes to maintain the integrity and stability of Indonesia's financial system while protecting customers from the losses caused by the increasingly sophisticated banking crimes.[9]

In facing the evolution of banking crimes, one of the key research questions is how the role of the Financial Services Authority (OJK) can effectively formulate policies and regulations to prevent and address banking crimes in the digital era. The development of technology and digitalization in the banking sector has opened up opportunities for the emergence of various new types of crimes, such as cybercrime, online fraud, and data theft. Therefore, OJK needs to design adaptive policies and regulations that not only maintain the stability of the financial system but also provide maximum protection to customers from these increasingly sophisticated threats.[10]

Additionally, another research question is regarding the various modes of banking crimes that have evolved with technological advancements and how OJK can adapt its supervisory strategies to face these threats. As digital transformation accelerates, banking crimes are becoming more diverse, ranging from online fraud to cyber-attacks that can hack banking systems. To address this, OJK must be able to identify emerging crime modes and develop more effective and responsive supervisory strategies in order to mitigate the risks posed and maintain public trust in the banking sector in Indonesia.

The research method used to analyze the strategies of the Financial Services Authority (OJK) in addressing the evolution of banking crimes in the digital era adopts a qualitative approach with various techniques, such as case studies, document analysis, in-depth interviews, and observation. The qualitative approach is chosen to deeply explore the phenomena occurring in the increasingly digitalized and complex banking world, as well as to understand how OJK's policies and regulations can address these emerging threats. In this study, case studies are used to analyze the steps taken by OJK in dealing with banking crime cases, both in Indonesia and abroad, to identify the successes and shortcomings of existing policies. Document analysis will be carried out by reviewing various regulations and official reports issued by OJK, such as policies on digital security, personal data protection, and supervision of the banking sector, to assess how effective these regulations are in addressing increasingly sophisticated threats. In-depth interviews with various stakeholders, such as OJK officials, bank representatives, cybersecurity experts, and practitioners in the financial industry, will be conducted to gain deeper insights into the implementation of policies and the challenges faced in combating banking crimes. Additionally, direct observation of the supervisory activities carried out by OJK and how banks and financial institutions implement digital security policies will also be conducted. The data collected from interviews, case studies, and document analysis will be analyzed using an inductive approach and content analysis techniques to identify patterns and key themes that emerge, in order to draw relevant conclusions. Ultimately, this research aims to provide policy recommendations that can enhance OJK's effectiveness in addressing the evolving banking crime threats and maintaining the stability of Indonesia's financial system in the future.[11]

[9] Keuangan, O. J. (2017). Otoritas Jasa Keuangan. *Salinan Peraturan Otoritas Jasa Keuangan Nomor*, *65*.
[10] Linggoraharjo, V. (2020). Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming. *Jurnal Magister Hukum ARGUMENTUM*, *7*(1), 34-46.
[11] Maulidya, G. P., & Afifah, N. (2021). Perbankan dalam era baru digital: menuju bank 4. 0. In *Proceeding Seminar Bisnis Seri V* (pp. 278-288).

Discussion

The discussion on the strategies of the Financial Services Authority (OJK) in addressing the evolution of banking crimes in the digital era is crucial for understanding how the regulations and policies implemented can protect the banking system, customers, and the entire financial sector from the increasingly complex threats. The first research question is related to how OJK plays a role in formulating effective policies and regulations to prevent and tackle banking crimes in the digital era. With the rapid advancement of digital technology in the banking sector, threats to the financial system have become more diverse and sophisticated. In this context, OJK acts as a regulator and supervisor, tasked with creating policies that not only keep pace with technological advancements but also ensure that these policies can address various emerging banking crimes.[12] For example, the rise of cybercrime involving the hacking of banking systems, online fraud carried out via digital media, and personal data theft that can be used for illegal transactions. These crimes require a rapid response and adaptive policies from OJK to mitigate the risks they pose. Therefore, OJK must design policies that ensure maximum protection for customers and the banking sector, while also strengthening regulations related to digital security systems, personal data protection, and oversight of financial institutions.

One of the steps taken by OJK is the introduction of stricter regulations on digital security, such as requiring financial institutions to implement advanced security technologies. For instance, the introduction of two-factor authentication (2FA) aims to enhance protection for access to customer accounts, as well as the use of data encryption to safeguard personal information from potential hacking threats. However, this policy should not only be implemented within financial institutions but must also cover a broader oversight system to monitor and address cybercrimes in the banking world. Thus, OJK not only plays a role in formulating effective regulations but must also conduct regular evaluations of the implementation of these policies to ensure they remain relevant in the face of rapid technological changes. One of the greatest challenges is to create policies that are flexible and adaptive, given that banking crimes continually innovate and develop more sophisticated modus operandi, such as the increasing prevalence of ransomware attacks in the banking sector.[13]

The second research question focuses on how OJK can identify and address the various banking crime modus operandi that are developing with technological advancements. These increasingly sophisticated crimes, such as cybercrime, online fraud, and personal data theft, require more precise oversight strategies. These crimes are often difficult to detect as they are carried out using digital technology, which is harder to monitor with traditional surveillance systems. Therefore, OJK needs to develop a more responsive, technology-based oversight strategy to detect and address these threats early on. One approach could involve increasing monitoring of suspicious digital transactions and introducing early warning systems capable of identifying potential fraud or ongoing cyberattacks.[14]

Additionally, OJK must strengthen its collaboration with various parties, both nationally and internationally, to combat banking crimes that are often transnational. This cooperation involves the exchange of information about emerging modus operandi and efforts to create more effective mitigation mechanisms. Collaboration with institutions like Bank Indonesia, the police, and even international organizations such as Interpol is essential in addressing the increasingly complex banking crimes that involve multiple parties. In this regard, OJK also needs to strengthen the reporting system for both customers and banks so that cases of fraud or cyberattacks can be reported quickly and followed up

[12] Mutiasari, A. I. (2020). Perkembangan industri perbankan di era digital. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *9*(2), 32-41.

[13] Ngamal, Y., & Perajaka, M. A. (2022). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59-74.

[14] Pikahulan, R. M. (2020). Implementasi fungsi pengaturan serta pengawasan pada Bank Indonesia dan Otoritas Jasa Keuangan (OJK) terhadap perbankan. *Jurnal Penegakan Hukum Dan Keadilan*, *1*(1), 41-51.

promptly. With strong collaboration among institutions, OJK can be more effective in formulating policies that ensure the security of the banking sector and protect customers from evolving threats.[15]

It is important to note that, in addition to policies and oversight strategies, OJK also has the responsibility to enhance public literacy and awareness of banking crimes. In addressing crimes that leverage advanced digital technologies, OJK must ensure that the public, particularly customers, understand how to protect their personal information and identify potential fraud or threats from the digital world. Therefore, the educational programs launched by OJK are crucial, as they provide the public with a better understanding of the importance of safeguarding personal data and recognizing the increasingly diverse digital fraud schemes.[16]

Overall, this discussion shows that OJK faces significant challenges in maintaining the stability of Indonesia's banking sector. To this end, OJK must formulate comprehensive and adaptive policies that not only secure the banking sector but also provide maximum protection to customers and raise public awareness. By strengthening regulations, enhancing technology-based oversight, and expanding collaboration with relevant parties, OJK can be more effective in addressing the evolution of banking crimes and maintaining the integrity and stability of Indonesia's financial system in the future.[17]

One of the primary regulatory frameworks OJK has implemented in response to the growth of digital banking and associated threats is the Regulation of the Financial Services Authority No. 77/POJK.01/2016 concerning Information Technology Governance for Financial Services Institutions. This regulation aims to ensure that financial institutions adopt robust digital security practices. The regulation requires financial institutions to establish strong internal controls, including comprehensive risk management systems and protocols for data security, which are critical in preventing cybercrimes such as hacking and unauthorized access to financial systems. The enforcement of these regulations aligns with global practices and is part of a broader strategy to safeguard customer data and maintain trust in the financial system.[18]

Another regulation that plays a key role is the Regulation of the Financial Services Authority No. 13/POJK.02/2018 on the Protection of Consumer Financial Services. This regulation sets the foundation for consumer protection within the financial services sector, particularly by establishing clearer guidelines for handling customer complaints, ensuring transparency in financial services, and providing a framework for resolving disputes. The regulation also mandates that financial institutions implement data protection measures that comply with the principles of transparency, security, and accountability.

Furthermore, OJK has integrated the General Data Protection Regulation (GDPR)-inspired policies, which align with Indonesia’s data protection efforts, enhancing personal data protection for banking customers. This regulatory framework mandates that financial institutions not only implement data security systems but also adhere to strict data collection, processing, and retention rules. These regulations are crucial in addressing crimes such as data theft, identity theft, and fraud, ensuring that personal information is not misused by cybercriminals.[19]

[15] Pulungan, M. R. (2019). *Kebijakan Otoritas Jasa Keuangan (OJK) Dalam Menghindari Tindak Pidana Perbankan Syariah Di Indonesia* (Doctoral dissertation, Universitas Islam Negeri Sumatera Utara).

[16] Purwanto, S., & Perkasa, D. H. (2024). ANALISIS TRANSFORMASI BANK DIGITAL YANG TERDAFTAR DI BURSA EFEK INDONESIA. *Jurnal Revenue: Jurnal Ilmiah Akuntansi*, *4*(2), 622-633.

[17] Ramadhan, T., & Purwandari, B. (2023). Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital Di Indonesia Guna Mencegah Social Engineering. *Syntax Idea*, *5*(1), 86-98.

[18] Sari, A. A. (2018). Peran Otoritas Jasa Keuangan Dalam Mengawasi Jasa Keuangan Di Indonesia. *Supremasi: Jurnal Hukum*, *1*(1), 23-33.

[19] Sormin, S. K., Vikri, M., & bin Darda, M. (2023). Kurangnya Nasabah Di Bank Syariah Dibandingkan Bank Konvensional. *Karimah Tauhid*, *2*(4), 1080-1086.

OJK has also mandated the use of advanced digital security technologies to strengthen banking systems against increasingly sophisticated cyber-attacks. One of the key regulatory requirements in this regard is the Two-Factor Authentication (2FA) for online banking services. This is a critical step to protect customer accounts from unauthorized access by requiring two forms of identification (e.g., a password and a fingerprint, or a password and an OTP sent to the customer's mobile device). 2FA has become a fundamental regulation for reducing the risk of unauthorized access to accounts, a key component in combatting phishing, account takeover, and other forms of cybercrime.[20]

Additionally, OJK's focus on data encryption is another regulatory measure that aims to secure sensitive customer data during digital transactions. Encryption ensures that data transmitted between banking platforms and customers remains private and cannot be intercepted by cybercriminals. This regulatory framework not only protects customer information but also addresses threats such as man-in-the-middle attacks and data breaches.[21]

Despite the comprehensive regulatory measures already in place, challenges remain due to the dynamic nature of digital threats. The rapid pace of technological development often outstrips the ability of regulations to keep up. For example, new forms of ransomware attacks and more sophisticated phishing schemes continuously emerge, which require a level of flexibility and innovation in OJK's approach to regulatory oversight. To overcome these challenges, OJK must ensure that its regulations are periodically updated and that financial institutions remain vigilant in adopting the latest security technologies.[22]

One recommendation is for OJK to increase collaboration with other regulatory bodies internationally. As banking crimes, particularly cybercrime, often transcend national borders, international cooperation is essential. OJK could improve information sharing with other financial regulators, law enforcement agencies, and international organizations like Interpol. This collaboration would help track emerging crime trends and implement rapid-response measures when cross-border financial threats occur.

Another recommendation is to enhance financial literacy programs for the public, specifically in digital banking security. While regulatory frameworks are critical for financial institutions, the success of these measures also depends on consumers' ability to protect their own data and detect fraud. Educating customers about online security practices, such as recognizing phishing emails or avoiding public Wi-Fi networks for financial transactions, could greatly reduce the risk of falling victim to digital banking crimes.

Conclusion

In conclusion, OJK has taken several proactive steps to regulate and supervise the banking sector in response to the rise of banking crimes in the digital era. Through regulations that enforce digital security, data protection, and consumer rights, OJK aims to secure the financial system and protect customers from increasingly sophisticated criminal activities. However, to remain effective, these regulations must be continually updated to address emerging threats, such as ransomware and phishing, and be accompanied by comprehensive strategies that include increased international collaboration and public education. By strengthening both regulatory frameworks and public awareness, OJK can help maintain a secure and trustworthy banking environment in Indonesia.

[20] Syafa, A. S. A., & Santoso, I. B. (2024). Modus Operandi Kejahatan Skimming Terhadap Nasabah Berdasarkan Perspektif Hukum Perbankan. *Jurnal Ilmiah Wahana Pendidikan*, *10*(8), 187-194.

[21] Syafitri, I. (2021). Perlindungan Konsumen Industri Asuransi Oleh Otoritas Jasa Keuangan. *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, *4*(2), 307-319.

[22] Wahjono, S. I. (2022). Pengertian FINTEK. *Publisher: Researchgate. Sentot Imam Wahjono*.

References

Anggoro, S. B., Amrullah, A., Tanuwijaya, F., & Anggono, B. D. (2024). Perbandingan Sistem Penegakan Hukum Kejahatan Perbankan di Era Digital di Negara Maju Dan Berkembang. *Syntax Literate; Jurnal Ilmiah Indonesia*, *9*(10), 5381-5391.

Aprita, S. (2021). Kewenangan Otoritas Jasa Keuangan (OJK) Melakukan Penyidikan: Analisis Pasal 9 Huruf C Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan. *Jurnal Ilmiah Universitas Batanghari Jambi*, *21*(2), 550-563.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *2*(1), 01-16.

Cholik, C. A. (2021). Perkembangan teknologi informasi komunikasi/ICT dalam berbagai bidang. *Jurnal Fakultas Teknik UNISA Kuningan*, *2*(2), 39-46.

Diba, N. F., Disemadi, H. S., & Prananingtyas, P. (2020). Kebijakan Tata Kelola Otoritas Jasa Keuangan (OJK) Di Indonesia. *Ekspose: Jurnal Penelitian Hukum dan Pendidikan*, *18*(2), 868-876.

Diba, N. F., Disemadi, H. S., & Prananingtyas, P. (2020). Kebijakan Tata Kelola Otoritas Jasa Keuangan (OJK) Di Indonesia. *Ekspose: Jurnal Penelitian Hukum dan Pendidikan*, *18*(2), 868-876.

Ekayani, L., Djanggih, H., & Suong, M. A. A. (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan. *Journal of Lex Philosophy (JLP)*, *4*(1), 22-40.

Fachrurrazy, M., & Siliwadi, D. N. (2020). Regulasi Dan Pengawasan Fintech Di Indonesia: Persfektif Hukum Ekonomi Syariah. *Al-Syakhshiyyah Jurnal Hukum Keluarga Islam dan Kemanusiaan*, *2*(2), 154-171.

Fadlan, A. F. (2022). *Bank dan lembaga keuangan lainnya*. Publica Indonesia Utama.

Keuangan, O. J. (2017). Otoritas Jasa Keuangan. *Salinan Peraturan Otoritas Jasa Keuangan Nomor*, *65*.

Linggoraharjo, V. (2020). Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming. *Jurnal Magister Hukum ARGUMENTUM*, *7*(1), 34-46.

Maulidya, G. P., & Afifah, N. (2021). Perbankan dalam era baru digital: menuju bank 4. 0. In *Proceeding Seminar Bisnis Seri V* (pp. 278-288).

Mutiasari, A. I. (2020). Perkembangan industri perbankan di era digital. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *9*(2), 32-41.

Ngamal, Y., & Perajaka, M. A. (2022). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59-74.

Pikahulan, R. M. (2020). Implementasi fungsi pengaturan serta pengawasan pada Bank Indonesia dan Otoritas Jasa Keuangan (OJK) terhadap perbankan. *Jurnal Penegakan Hukum Dan Keadilan*, *1*(1), 41-51.

Pikahulan, R. M. (2020). Implementasi fungsi pengaturan serta pengawasan pada Bank Indonesia dan Otoritas Jasa Keuangan (OJK) terhadap perbankan. *Jurnal Penegakan Hukum Dan Keadilan*, *1*(1), 41-51.

Pulungan, M. R. (2019). *Kebijakan Otoritas Jasa Keuangan (OJK) Dalam Menghindari Tindak Pidana Perbankan Syariah Di Indonesia* (Doctoral dissertation, Universitas Islam Negeri Sumatera Utara).

Purwanto, S., & Perkasa, D. H. (2024). ANALISIS TRANSFORMASI BANK DIGITAL YANG TERDAFTAR DI BURSA EFEK INDONESIA. *Jurnal Revenue: Jurnal Ilmiah Akuntansi*, *4*(2), 622-633.

Ramadhan, T., & Purwandari, B. (2023). Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital Di Indonesia Guna Mencegah Social Engineering. *Syntax Idea*, *5*(1), 86-98.

Sari, A. A. (2018). Peran Otoritas Jasa Keuangan Dalam Mengawasi Jasa Keuangan Di Indonesia. *Supremasi: Jurnal Hukum*, *1*(1), 23-33.

Sormin, S. K., Vikri, M., & bin Darda, M. (2023). Kurangnya Nasabah Di Bank Syariah Dibandingkan Bank Konvensional. *Karimah Tauhid*, *2*(4), 1080-1086.

Syafa, A. S. A., & Santoso, I. B. (2024). Modus Operandi Kejahatan Skimming Terhadap Nasabah Berdasarkan Perspektif Hukum Perbankan. *Jurnal Ilmiah Wahana Pendidikan*, *10*(8), 187-194.

Syafitri, I. (2021). Perlindungan Konsumen Industri Asuransi Oleh Otoritas Jasa Keuangan. *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, *4*(2), 307-319.

Wahjono, S. I. (2022). Pengertian FINTEK. *Publisher: Researchgate. Sentot Imam Wahjono*.