JILPR Vol. 6, No. 2 February 2025
Journal of Indonesia Law & Policy Review 2715-498X

IMPLEMENTATION OF CRIMINAL SANCTIONS AGAINST PERPETRATORS OF BANK ACCOUNT DATA THEFT THAT IS FAIR FOR THE PUBLIC

Raden Jossy Sutari Belgradoputra[1*], Waty Suwarty Haryono[2], Ali Johardi Wirogioto[3]
[1,2,3]Faculty of Law, Krisnadwipayana University, Jakarta, Indonesia
jossie_bp@yahoo.com[1*], watysuwarty@gmail.com[2], alijohardi@gmail.com[3]

Abstract
The implementation of criminal sanctions against skimming offenders must be based on principles of justice that encompass the interests of victims, society, and offenders. This crime often results in significant financial losses and psychological impacts on victims, making it essential for the penalties imposed to reflect the extent of the harm caused. The theory of justice proposed by Gustav Radbruch, namely legal justice, social justice, and substantive justice, serves as a critical foundation for enforcing the law proportionally. Legal justice enforcement, as outlined in Articles 30 and 36 of the ITE Law, provides a framework to prosecute offenders with a maximum penalty of 12 years of imprisonment and fines up to IDR 12 billion. This ensures legal certainty while also deterring potential offenders. Social justice emphasizes collective protection for society, including safeguarding banking data. The state must ensure that banking systems have secure infrastructure so that the public is less vulnerable to cybercrime. Firm punishment of offenders also instills a sense of security in the community. Substantive justice must be realized by restoring victims' losses. Punishment for offenders should not only involve imprisonment but also include mechanisms for restitution to recover victims' material losses. Integrating these three principles ensures that the implementation of criminal sanctions is not merely repressive but also restores a sense of justice in society. This approach is necessary to maintain a balance between punishing offenders, protecting society, and upholding the rights of victims.

Keywords : Theft, cybercrime, justice

INTRODUCTION

Bank data theft, especially targeting customer accounts, is on the rise. This crime, often committed by foreigners but also by Indonesian citizens, is essentially conventional theft executed using computers. Despite being a computer-related crime, the penalties stipulated in the Criminal Code often seem inadequate.

The lenient sentences handed down to perpetrators, often just one year minus time served, raise concerns about the effectiveness of our justice system. Judges face a unique challenge in sentencing these cases, as they cannot solely rely on the Electronic Information and Transaction (ITE) Law. The relatively mild punishments do little to deter criminals and fail to align with the objectives of criminal justice.

Experts argue that the penalties under the ITE Law are too lenient and fail to serve as a deterrent. Perpetrators often receive only short prison sentences or small fines compared to the losses suffered by victims. The legal procedures and evidence requirements in data theft cases are often insufficient, leading to inadequate punishments.

Given the significant harm caused by bank data theft or skimming, the aggravating element of money laundering, as defined in Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering, should be considered. This law stipulates heavier penalties for crimes involving the proceeds of various offenses, including corruption, bribery, and drug trafficking.

The emergence of cybercrimes has created widespread public concern, necessitating comprehensive legal reforms, particularly in criminal law. The crimes most prevalent in the modern era are data theft, both personal and financial. This paper aims to examine bank data theft, specifically the practice of skimming ATMs, and to propose recommendations for more effective legal reforms.

Bank data theft falls under the category of special crimes as stipulated in Article 32 paragraph (2) of Law Number 11 of 2008 on Electronic Information and Transactions, although it is not explicitly defined in the Criminal Code. Violations of this article carry the penalties outlined in Article 48 of the same law. Bank data theft typically involves a criminal syndicate. While the basic form of theft is defined in Article 362 of the Criminal Code, the concept of theft has evolved with the times.

A review of several bank data theft cases reveals that the sentences imposed by judges are relatively lenient, failing to deter future crimes. Article 48 of the ITE Law stipulates a maximum prison sentence of nine years and/or a maximum fine of Rp 3 billion. However, these penalties often prove inadequate.

RESEARCH METHODS

This research is a normative juridical legal research, because the researcher only uses secondary data. The normative approach focuses on research on regulations, doctrines, and legal principles, by collecting various materials from legal practices, namely several court decisions to be studied. The approaches used are as follows: (a) legislation (statute approach) which studies various provisions in legislation; (b) conceptual approach which examines legal principles regarding criminal sanctions against perpetrators of bank account data theft; while (c) case approach which describes and analyzes cases with relatively light sentences.

RESULT AND DISCUSSION

Perspectives on Bank Account Data Theft in Indonesia

Perpetrators of bank account data theft in Indonesia employ various methods to gain illegal access to financial information. Some common methods used in cybercrime in the banking sector include:

a) Phishing Cybercrime

This term is derived from "fishing," which means to lure information. Phishing also means enticing internet users to provide personal data and passwords on compromised websites. Typically, these attacks target online banking users (Munir, 2009). In general, this crime is carried out by perpetrators by sending emails or messages that appear to be from trusted sources, such as banks or financial institutions, to deceive victims into providing their personal information, including account numbers and passwords.

b) Skimming Cybercrime
This is the act of stealing credit or debit card information by illegally copying data from the card's magnetic strip. This strip is used to store customer data (Mansur & Gultom, 2005).

c) Malware Cybercrime: Malware is malicious software that damages or exploits devices and networks. Cybercriminals use it to steal valuable data, such as financial data and passwords. Malware includes viruses and is used for various purposes.

Impact of Bank Account Data Theft Bank account data theft has a significant impact on victims, including:

a) Financial Loss
Victims lose a sum of money from their accounts due to unauthorized transactions. In some cases, the entire account balance can be drained before the victim is aware of any suspicious activity.

b) Emotional Loss
In addition to financial loss, victims also experience stress and anxiety due to losing money and the often complicated and time-consuming recovery process.

c) Reputation Loss
For businesses or companies, bank account data theft can damage their reputation in the eyes of customers and business partners, which in turn can affect overall business performance.

Data on Perpetrators of Cybercrime in the Banking Sector

Bank data theft, commonly referred to as skimming, has been ongoing since 2009. Essentially, bank data theft occurs in the digital realm, where no tangible items are physically transferred. According to Nuzulla Agustina, data can be defined as information about something that has occurred frequently and consists of a series of numbers, facts, images, tables, graphs, words, symbols, letters, and others that express a thought, condition, or situation.

Table 1. Court Decision Case Data 2019 – 2021

No	Decision number	Criminal Penalties	Nationality of the Defendant
1	60/Pid.Sus/2019/PNLbj	2 years in prison, 200 million fine	Mihail Staykov Georgiev aka Mihail, citizen Bulgaria
2	88/Pid.Sus/2019/PNKds	2 years in prison, 50 million fine	Rasaiah Satheeskumar bin Rasaiah, citizen Sri lanka
3	256/Pid.Sus/2019/PNDps	8 months in prison, 2 million fine	Vasil Kostadinov Nikolov, Dupnitsa
4	258/Pid.Sus/2019/PNDps	8 months in prison, 2 million fine	Vladimir Vladimirov Cholakov, citizen Bulgaria
5	439/Pid.Sus/2019/PNDps	8 months in prison, 5 million fine	Ivaylo Filifo Trifonnov; George Jordanov Jordanov aka George; Todor Krasimirov Dobrev, citizen Bulgaria
6	440/Pid.Sus/2019/PNDps	8 months in prison, 2 million fine	Andrey Iliev Peychep; Varadin Nikolaev Popov, WN Bulgaria
7	639/Pid.Sus/2019/PNDps	8 months in prison, 25 million fine	Alin Serdaru, citizen Rumania

8	640/Pid.Sus/2019/PNDps	7 months and 8 months in prison, 25 million baht fine	Alisa Sardaru and Sorin Velcu, citizen Rumania
9	707/Pid.Sus/2019/PNDps	8 months in prison, 5 million fine	Kaloyan Kirilov Spasov; Lyubomir Todorov Bogdanov; Nikolay Valentinov Dinev als Niki; Valentin Chavdarov Galchev, citizen Bulgaria
10	1258/Pid.Sus/2019/PNDps	8 months in prison, 2 million fine	Stoyanov Georgi Ivanov, citizen Bulgaria
11	1511/Pid.Sus/2019/PNDps	7 months in prison, 5 million fine	Roman Vakal, citizen Ukraina
12	163/Pid.Sus/2020/PNNgw	1 year 10 months in prison, 10 million baht fine	Saryanto Aladam bin Sajuri, Tri Warno Bin Karmono, citizen Indonesia
13	168 /Pid.Sus/2020/PN Mtr	3 years and 6 months in prison, 100 million baht fine	Yunus Emrek Senbayik aka Emre, citizen Turki
14	334/Pid.Sus/2020/PN Mlg	1 year in prison, 5 million fine	Rizal Yanuar, Dani Mahendra, Predi Suryadi, citizen Indonesia
15	762/Pid.B/2020/PNJkt.Utr	4 years in prison, 1 billion fine	Muhammad Rendra, Haldi, Dino Saputra aka H. Ibrahim Alias Paci, Arsaufi Aka Reza, seluruhnya citizen Indonesia
16	1045/Pid.B/2020/PNJKT.TIM.	2 years in prison, no fine	Hayrullah Ceylan, Ufuk Kemaneci, Hakan Battal, seluruhnya citizen Turki
17	239/Pid.Sus/2021/PN Dps	2 years and 6 months in prison, 100 million baht fine	Putu Rediarsa aka Putu, citizen Indonesia

Source: Directory of Decisions of the Supreme Court of the Republic of Indonesia (processed)

Table 1 data was obtained from the Directory of Decisions of the Supreme Court of the Republic of Indonesia in 2019-2021 regarding theft of banking data by skimming, among 17 (seventeen) decisions, 11 (eleven) decisions imposed an average sentence of between 7 months to 1 year 10 months in prison. 4 (four) decisions imposed a sentence of 2 years in prison, 1 (one) decision imposed a sentence of 3 years in prison, and 1 (one) decision imposed a sentence of 4 years in prison.

Crimes in the banking world can cause economic chaos, which according to Mardjono Reksodiputro, these crimes are economic crimes (Reksodiputro, 2020). This is evidenced by the rampant practice of theft that harms bank customers by stealing ATM card data information called skimming. The following is the value of customer losses:

Table 2. Customer Loss Value

No	Decision Number	Loss (Rupiah)	Description/ Customers who are harmed
1.	60/Pid.Sus/2019/PNLbj	4.700.000,-	ABDUL GHANI A
2.	256/Pid.Sus/2019/PN Dps	2.500.000,-	Allegedly proceeds of crime, confiscated for the state
3.	334/Pid.Sus/2020/PN Mlg	588.000.000.-	RISTIONO

4.	439/Pid.Sus/2019/PN Dps	51.000.000,-	BANK MANDIRI through witness Ida Bagus Darmawan, SE.
5.	440/Pid.Sus/2019/PNDps	130.000.000,- 557.000.000,-	Allegedly proceeds of crime, confiscated for the state
6.	639/Pid.Sus/2019/PNDps	5.600.000,-	Allegedly proceeds of crime
7.	707/Pid.Sus/2019/PNDps	7.500.000,- 110.000.000,- 700.000,-	BNI through I Nengah Ariyasa, SE. Allegedly proceeds of crime, confiscated for the State
8.	762/Pid.B/2020/PN Jkt.Utr	1.143.000.000,-	H. ABDUL RAHIM
9.	1258/Pid.Sus/2019/PNDps	6.200.000,-	BNI through I Nengah Ariyasa, SE. Allegedly proceeds of crime, confiscated for the State
10.	163/Pid.Sus/2020/PNNgw	36.000.000,-	Yudi Pramono

Source: Directory of Decisions of the Supreme Court of the Republic of Indonesia (processed)

The Application of Imprisonment for Cybercrimes in Banking

Advances in technology have not only benefited society but have also created new avenues for crime, particularly in the banking sector. The integration of online systems, such as e-money, e-cash, mobile banking, and e-banking, into the financial industry has made it susceptible to cyberattacks.

A prime example is Case Number 334/Pid.Sus/2020/PN Malang, which involved a cybercrime in the banking sector. The defendants, Rizal Yanuar, Dani Mahendra, and Predi Suryadi, were found guilty of violating Article 46 paragraph (3) in conjunction with Article 30 paragraph (3) of Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Electronic Information and Transactions, in conjunction with Article 55 paragraph (1) of the [1] Criminal Code and Article 64 paragraph (1) of the Criminal Code.

They were convicted of jointly accessing a computer and/or electronic system by hacking into a security system, considered a continuous offense. Their sentence was one year's imprisonment and a fine of Rp5,000,000 (five million rupiah), with a subsidiary punishment of two months' imprisonment if the fine was not paid.

The victims suffered a loss of Rp588,000,000 (five hundred eighty-eight million rupiah), a substantial amount that was disproportionate to the sentence handed down. The uniform sentence imposed on the defendants was inappropriate and did not reflect a sense of justice for both society and the defendants.

One oversight by both the public prosecutor in their indictment and the panel of judges in their verdict was the element of "harm to others" in Article 36 of Law No. 19 of 2016, which was clearly evident from the beginning of the investigation. This should have been considered an aggravating factor in sentencing.

Another example is Case Number 762/Pid.B/2020/PN Jkt.Utr, involving Muhammad Rendra, Haldi, Dino Saputra alias H. Ibrahim alias Paci, and Arsaufi alias Reza, all Indonesian citizens. They were each sentenced to four years' imprisonment and a fine of Rp1,000,000,000 (one billion rupiah), with a subsidiary punishment of six months' imprisonment if the fine was not paid.

In this case, the defendants used a fraudulent scheme, pretending to be Bruneian citizens selling a large number of mobile phones. They asked the victim to check their account balance using the victim's ATM card. The victim suffered a loss of Rp1,143,000,000 (one billion one hundred forty-three million rupiah).

The dominance of imprisonment as a criminal penalty in Indonesian law, according to Sudarto, is rooted in the term itself. The word "penjara" (prison) originates from the Javanese word "penjoro," meaning repentance or deterrence. Thus, imprisonment is intended to deter

individuals from committing crimes. Imprisonment as a form of punishment was introduced to Indonesia during the Dutch colonial period.

Regarding the sentencing of foreign nationals, the principle of territoriality is a fundamental principle in international law. Article 2 of the Indonesian Criminal Code states that criminal provisions apply to anyone who commits a crime in Indonesia. This principle is the basis for imposing penalties on foreign nationals who commit crimes within Indonesian territory.

In essence, Indonesian criminal law applies to crimes committed within Indonesian territory, regardless of the nationality of the perpetrator. This territorial principle is the legal basis for imposing penalties on foreign nationals who commit crimes in Indonesia.

Aggravating Circumstances in Criminal Law

The Indonesian Criminal Code (KUHP) includes provisions regarding aggravating circumstances, such as aggravating reasons and aggravating grounds. An aggravating reason is a condition that increases the severity of the penalty for a criminal act. For instance, in Article 338 of the KUHP, if someone is convicted of murder, which carries a 15-year prison sentence, a repeat offense can increase the sentence to 20 years. The difference between aggravating reasons and aggravating factors in a judgment is that the latter is a consideration for the judge, not a legal reason. Three common aggravating reasons are found in Articles 52, 52a, and 486, 487, and 488 of the KUHP.

Aggravating reasons can also be found outside the KUHP, as stipulated in specific laws. For example, Article 2 paragraph (2) of Law Number 31 of 1999, as amended by Law Number 20 of 2001 on Corruption, provides an example. Article 2 paragraph (1) of this law explicitly states that if a person commits an act in violation of the law to enrich themselves, others, or a corporation, thereby endangering the state's finances or economy, they shall be punished by life imprisonment or a minimum of four years and a maximum of twenty years imprisonment, with a minimum fine of Rp200 million and a maximum of Rp1 billion. Article 2 paragraph (2) is an aggravating circumstance, stating that: "In cases where the corruption crime as referred to in paragraph (1) is committed under certain circumstances, the death penalty may be imposed" (Santoso, 2023).

The "certain circumstances" here refer to "aggravating factors for perpetrators of corruption crimes, namely if the crime is committed against funds allocated for disaster management, national natural disasters, handling the consequences of widespread social unrest, handling economic and monetary crises, and the repetition of corruption crimes (Santoso, 2023)."

Skimming, the theft of banking data using tools or technology to illegally access bank account data, is a form of cybercrime with far-reaching implications. In Indonesian criminal law, aggravating circumstances in such cases can be analyzed from the provisions of Article 36 of the ITE Law (Electronic Information and Transaction Law) and Articles 3 and 4 of the Anti-Money Laundering Law.

The Implementation of Criminal Penalties for Bank Account Data Theft Considered Relatively Light Compared to Maximum Penalties

Criminal penalties under the Electronic Information and Transaction Law are often considered too lenient for perpetrators of bank account data theft. This is due to a lack of application of the principle of retributive justice, which should ensure that punishment fits the crime, especially those that cause significant harm to individuals. In reality, bank account data theft often results in substantial losses for victims, while the penalties imposed in some cases are limited to fines or relatively short prison sentences, which are disproportionate to the victims' suffering. For example, in Case Number 334/Pid.Sus/2020/PN Malang, the judge only imposed a one-

year prison sentence and a fine of Rp5,000,000 (five million rupiah), with a subsidiary punishment of two months' imprisonment if the fine was not paid. According to the law, the perpetrator could have been sentenced to a maximum of eight years imprisonment and/or a fine of no more than Rp800,000,000 (eight hundred million rupiah). The seven-year difference in the implemented penalty indicates that both the public prosecutor and the judge did not consider the element of harm to others as stipulated in Article 36 of the ITE Law.

In Case Number 762/Pid.B/2020/PNJkt.Utr, involving four Indonesian citizens, Muhammad Rendra, Haldi, Dino Saputra alias H. Ibrahim alias Paci, and Arsaufi alias Reza, they were each sentenced to four years imprisonment and a fine of Rp1,000,000,000 (one billion rupiah). In this case, the judge viewed it as a conventional crime of theft committed by two or more people, which carries a maximum prison sentence of seven years. As a result, the judge used the Criminal Code and the Anti-Money Laundering Law as aggravating factors in imposing the sentence. The victims suffered a loss of Rp1,143,000,000 (one billion one hundred forty-three million rupiah). This case involved a direct interaction between the perpetrator and the victim, where the perpetrator physically exchanged the victim's ATM card with a prepared card.

The Application of the Principle of Justice for Society in Bank Account Data Theft Cases in Indonesia

In the context of cyber law, information technology is a double-edged sword. On the one hand, it contributes to human progress and well-being. On the other hand, it can be used to facilitate criminal activities. Law and justice are inseparable, as justice is a fundamental concept in legal theory. Justice is the primary virtue of social institutions, just as truth is a system of thought.

Several theories of criminal law discuss retributive justice, proportional justice, and restorative justice. In the Indonesian criminal justice system, the application of the principle of justice by judges in cases of bank account data theft is closely related to the theory of justice proposed by Gustav Radbruch. His theory, known as the Triad Theory, consists of justice, legal certainty, and expediency.

These three principles must be balanced, but justice should be the primary priority in the application of the law, especially when a law has an unjust impact on society. Justice focuses on equal treatment for similar cases and the protection of individual rights, particularly to ensure that no party is disproportionately harmed by legal actions taken in court (Huijbers, 1982).

Radbruch further distinguished three important aspects of justice: legal justice, social justice, and substantive justice. These three principles can be used as a benchmark for assessing how justice is applied in court decisions on crimes involving digital data theft, which is increasingly prevalent in the digital age.

a) Legal Justice
   This focuses on the consistent application of positive law in accordance with existing regulations. In the context of bank account data theft, legal justice is applied when judges refer to the provisions stipulated in laws and regulations, such as Articles 30 and 32 of the ITE Law and the provisions of Article 363 of the Criminal Code if relevant to the case.
b) Social Justice
   Radbruch focused on the social impact of court decisions and how these decisions affect society. In cases of bank account data theft, this crime not only harms individuals but also has broader social implications, including a decline in public trust in digital banking systems and the security of personal data. In certain cases, sentences deemed too lenient can be considered a violation of the principle of social justice because they fail to provide a strong enough deterrent for perpetrators and potential offenders. Therefore, the imposed penalties should provide greater protection for society and emphasize the preventive aspect.
c) Substantive Justice

This emphasizes the fulfillment of inherent values of justice, where judicial decisions not only comply with formal legal rules but also consider broader justice for victims, perpetrators, and society. In the context of bank account data theft, the application of substantive justice by judges means considering the financial losses suffered by the victim, the psychological impact, and other intangible losses that may arise from the data theft. Judges must comprehensively evaluate whether the imposed penalty truly reflects the harm suffered by the victim and ensure that the perpetrator is held accountable for their actions.

CONCLUSIONS

Implement alternative punishments such as progressive fines, electronic monitoring, or community service for perpetrators of bank account data theft, especially for cases with less significant financial losses. This step can reduce the burden on correctional institutions while providing a deterrent effect.

Focus sanctions on efforts to restore victims' losses through restitution and compensation mechanisms. Perpetrators are required to pay compensation according to the losses incurred, so that the law provides direct justice for victims without increasing the burden on correctional institutions.

REFERENCES

Anonim. (2023, Juli 18). *Pengertian data: Fungsi, manfaat, jenis, dan contohnya.* Gramedia. https://www.gramedia.com/

Anwar, M. (1979). *Hukum pidana bagian khusus (Jilid 1).* Alumni.

Arief, D. M., Mansur, & Gultom, E. (2005). *Cyber law: Aspek hukum teknologi informasi.* Refika Aditama.

Huijbers, T. (1982). *Filsafat hukum dalam lintasan sejarah.* Kanisius.

McAfee. (2024, Juli 16). *Why do cybercriminals use malware?* https://www.mcafee.com/id-id/antivirus/malware.html

Munir, H. N. (2017). *Pengantar hukum siber Indonesia.* Rajawali Pers.

Rahmalia, N. (2024, Oktober 24). *Skimming: Definisi, modus, dan cara menghindarinya.* Glints. https://glints.com/id

Reksodiputro, M. (2020). *Sistem peradilan pidana.* Rajawali Pers.

Santoso, T. (2023). *Asas-asas hukum pidana.* Rajawali Pers.

Sihombing, T. (2020). Efektivitas penegakan hukum terhadap pencurian data di Indonesia. *Jurnal Kriminologi Indonesia, 11*(1), 45-58.

Sudarto, et al. (2023). *Guru besar Undip bicara pembaharuan hukum pidana.* Rajawali Pers.

Widodo. (2009). *Sistem pemidanaan dalam cyber crime; Alternatif ancaman pidana, kerja sosial dan pidana pengawasan bagi pelaku cyber crime.* Aswaja Pressindo.

Zubair, S. (2019). Analisis sanksi pidana terhadap kejahatan siber dalam UU ITE: Studi kasus pencurian data. *Jurnal Hukum dan Teknologi, 5*(2), 123-134.