KOLABORASI
JOURNAL OF MULTIDISCIPLINARY
ACADEMIC SOLUTION PUBLISHER

Juridical Analysis of Cybercrime Carding: Crime of Credit Card and ATM Data Manipulation in Legal Perspective

Sarles Gultom[1], Van Lodewijk Purba[2], Anggun Pasaribu[3]

[1, 2, 3] *Universitas Simalungun, Indonesia*
**Corresponding Author*: sarlesgultomlawyer@gmail.com

Article Info

Article history:

Received :
Accepteance :
Published :
Available online
http://aspublisher.co.id/index.php/kolaborasi

E-ISSN: 3064-4054

How to cite:
Gultom. S., Purba, L, V., Pasaribu, A (2025). "Juridical Analysis of Cybercrime Carding: Crime of Credit Card and ATM Data Manipulation in Legal Perspective". KOLABORASI: Journal Of Multidisciplinary, vol. 2, no. 1, pp. 16-24, 2025.

ABSTRACT

Cybercrime carding, which involves the manipulation of credit card or ATM data, has frequently occurred in Indonesia and has gained significant international attention due to the risks associated with the misuse of technology in the digital information era. Several key issues require examination, including the factors causing cybercrime data manipulation, the modus operandi of cybercrime carding offenses, and the challenges and efforts in addressing this crime. The study, conducted using a library research method, concludes that cybercrime carding is driven by various factors such as rapid technological advancement, individuals testing their internet technology skills, socio-economic conditions, technical vulnerabilities, weak banking supervision systems, user negligence, inadequate network security, and lack of control by society and law enforcement agencies. The modus operandi of cybercrime carding includes Unauthorized Access to Computer Systems and Services, Illegal Content, Data Forgery, Cyber Espionage, Cyber Sabotage and Extortion, Offenses against Intellectual Property, and Infringements of Privacy. However, legal enforcement faces significant obstacles, including inadequate legal frameworks, limited investigative capabilities, insufficient evidence, and a lack of forensic computing facilities. One of the current efforts to combat cybercrime, including carding, is the formulation of the Draft Law on Electronic Information and Transactions (RUU ITE), which aims to establish comprehensive legal provisions for addressing cybercrime offenses in Indonesia.

Keywords: *Cybercrime Carding, Credit Card and ATM Data Manipulation, Legal Enforcement in Cybercrime Prevention.*

1. INTRODUCTION

The rapid development of information technology and digital transactions has significantly influenced financial activities, including the increasing use of credit cards and Automated Teller Machines (ATMs) (Anifowose & Ekperiware, 2022;

Javaid et al., 2022). However, this digital progress has also opened opportunities for cybercriminals to commit fraud and financial crimes, one of which is carding—a form of cybercrime that involves the illegal use of stolen credit card or ATM data for unauthorized transactions (Stojkovic et al., 2023; Katarina et al., 2023). According to cybersecurity reports, carding has become one of the most frequent financial cybercrimes worldwide, resulting in billions of dollars in losses annually (Maluleke, 2023; Bhanawat & Khang, 2024). Criminals use various techniques, including phishing, skimming, malware attacks, and hacking, to obtain sensitive payment information, which they then exploit to conduct fraudulent transactions (Nicholls et al., 2021; Kumar, 2023). The increasing prevalence of this crime has raised concerns among financial institutions, law enforcement, and consumers, necessitating stricter regulatory measures to combat cybercrime effectively.

Legal scholars and cybersecurity experts have studied carding as a sophisticated cybercrime that exploits vulnerabilities in digital payment systems (Alkhalil et al., 2021; Sogenbits & Turksen, 2024). According to Solms & Niekerk (2013), cybercrime, including carding, thrives due to the anonymity and global reach of the internet, making it difficult for law enforcement agencies to track and prosecute offenders. Various legal frameworks have been implemented to address cybercrime, including the Budapest Convention on Cybercrime 2001 and Indonesia's Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later revised by Law No. 19 of 2016. Article 30 of the ITE Law criminalizes unauthorized access to electronic systems, while Article 32 prohibits data manipulation and electronic fraud. Additionally, Indonesia's Criminal Code (KUHP) and Law No. 3 of 2011 on Fund Transfers also provide legal protection against electronic fraud, including carding activities. Despite these legal instruments, cybercriminals continue to evolve their methods, highlighting the need for more effective enforcement and international cooperation to combat this form of financial crime.

This study aims to analyze the legal framework and law enforcement mechanisms related to cybercrime carding, particularly in the context of credit card and ATM data manipulation. The research will explore the effectiveness of Indonesia's existing cyber laws in addressing and preventing carding crimes and compare them with international standards. Furthermore, this study seeks to identify gaps in law enforcement practices and propose recommendations to strengthen legal measures against cybercriminals. The analysis will focus on how financial institutions, government agencies, and law enforcement collaborate to prevent and mitigate cyber fraud, as well as examine challenges faced in prosecuting cybercriminals operating across multiple jurisdictions.

Despite the existence of legal provisions addressing cybercrime, the enforcement of laws against carding remains insufficient due to jurisdictional limitations, lack of forensic expertise, and the anonymity of cybercriminals. This study hypothesizes that Indonesia's legal framework on cybercrime needs further enhancement through stricter regulations, better technological security measures, and improved collaboration between law enforcement agencies and financial institutions. Strengthening cybersecurity infrastructure, increasing public awareness about online fraud, and implementing advanced fraud detection mechanisms are crucial to reducing the prevalence of carding. Furthermore, international cooperation and extradition treaties play a pivotal role in apprehending cybercriminals who operate beyond national borders. The findings of this study are expected to contribute to legal discourse and policy-making efforts aimed at developing a more robust legal and institutional framework to combat cybercrime in Indonesia.

2. RESEARCH METHOD

This study employs a qualitative descriptive method to produce an academic work that is educational for both the academic community and the general public. This approach aims to systematically analyze and interpret data by selectively and critically considering relevant references. The research emphasizes objectivity and scientific integrity to ensure the validity and efficiency of an academic work based on reliable legal sources, theories, and previous research findings (Neuman, 2014). By utilizing this approach, the study not only reveals legal facts related to the examined phenomenon but also examines normative aspects associated with regulations and law enforcement implementation against cybercrime carding in Indonesia. Data collection is conducted through library research, referring to statutory regulations, jurisprudence, and relevant academic literature (Creswell, 2018).

3. RESULT AND ANALYSIS

Factors Causing Cybercrime Data Or Atm Manipulation

The development and use of the internet has significantly changed the behavior of individuals, society, government, and the business world in interacting, communicating, transacting, and distributing information. The ease and speed of internet access triggers behavioral changes that have positive impacts, such as effectiveness, business efficiency, and increased competitiveness. However, the use of the internet also carries risks, including increasing cybercrime, one of which is carding, a crime related to the illegal manipulation of credit card or ATM data (Manaf, 2023; Sinaga, 2023). The phenomenon of carding cybercrime is increasingly receiving widespread attention, especially because of its impact on the banking system and public trust in digital transactions.

Factors that cause the rise of carding cybercrime include several aspects, including: (1) Technical factors, where rapid advances in information technology create security gaps that can be exploited by cybercriminals; (2) Socio-economic factors, where economic incentives encourage individuals to use technology as a tool of crime; (3) Technological development factors, which enable a borderless world and facilitate carding crimes through cross-border transactions; (4) Weak banking supervision system factors, which allow perpetrators to exploit weaknesses in bank security systems; and (5) The negligence factor of internet users, where the lack of awareness of the importance of network security systems makes individuals vulnerable to theft of personal data (Perwej et al., 2021).

The modus operandi of carding cybercrime includes several forms, including unauthorized access, data forgery, cyber espionage, cyber sabotage, and offense against intellectual property. Carding perpetrators often use techniques such as phishing, keylogging, or skimming to obtain users' credit card or ATM information without permission. Several carding cases that have occurred in Indonesia include credit card hacking via the internet, embezzlement of money via computers at Bank BRI Yogyakarta, and credit card hacking at BNI 46 New York branch (Saputra, 2022). The weak digital banking security system and increasing access to hacking tools have further exacerbated this condition (Aslan et al, 2023).

In efforts to combat carding cybercrime, there are several major obstacles that need to be overcome, including (1) Lack of comprehensive legal instruments, where the Electronic Information and Transactions Law (UU ITE) Number 19 of 2016 has not fully accommodated all forms of cybercrime; (2) Lack of resources in law enforcement, both in terms of the number of investigators, understanding of technology, and limited digital evidence; and (3) Lack of public awareness, where internet users still do not understand how to protect their personal data from cybercrime (Marune & Hartanto, 2021). Therefore, efforts to combat carding cybercrime need to be carried out through a comprehensive approach, including strengthening regulations, increasing the capacity of law enforcement in the field of digital forensics, and increasing public awareness and digital literacy.

Modus Operandi Of Data Manipulation Crimes, Both Online And Offline

Cybercrime is a form of modern crime that is developing along with the rapid development of information technology. One of the most common forms of cybercrime is carding, which is the manipulation of credit card or ATM data to gain illegal profits. The modus operandi used by carding perpetrators is increasingly complex, both through online and offline methods (Arief, 2020).

1. Online Carding Crime Modus Operandi

Carding crimes committed online exploit information system security gaps and lack of user awareness. Some common modus operandi found in online credit card or ATM data manipulation crimes include:

1) Unauthorized Access to Computer System and Service: Illegal access to a computer network system without permission with the aim of stealing or changing sensitive data (Mubeen et al., 2022).
2) Illegal Contents: The spread of false or illegal information on the internet that can harm other parties, such as the spread of fake news to deceive customer.

3) Data Forgery: Falsification of data on digital documents to carry out illegal transactions using stolen credit cards.
4) Cyber Espionage: Espionage actions via the internet by illegally accessing the banking system to obtain sensitive customer information.
5) Cyber Sabotage and Extortion: Hacking the banking system by spreading viruses, malware, or ransomware to obtain illegal profits.
6) Offense Against Intellectual Property: Theft of intellectual property rights in cyberspace, such as illegal use of credit card identities.
7) Infringements of Privacy: Theft of someone's personal information such as credit card numbers, ATM PINs, and other financial data for criminal purposes.

2. Offline Carding Crime Modus Operandi

In addition to online methods, carding can also be done offline by exploiting weaknesses in the banking system and customer ignorance. The modus operandi that is often used includes:

1) Customer Data Purchase: Customer data is traded by bank officials at relatively low prices (Rahman, 2020).
2) Telephone Fraud: The perpetrator contacts the victim by claiming to be from the bank and offers a credit card package upgrade service.
3) Fake Courier Delivery: The perpetrator sends a courier to collect the victim's personal information, such as photocopies of ID cards and credit cards.
4) Credit Card Duplication: After obtaining the victim's data, the perpetrator makes a duplicate credit card and uses it for illegal transactions.
5) Destruction of Fake Credit Cards: The perpetrator hands over a new credit card to the victim and cuts up the old credit card, but the card that is destroyed is actually a fake card, while the original card is misused by the perpetrator (Suryanto, 2021).

Carding crimes can be categorized as transnational crimes based on Article 3 paragraph (2) of the United Nations Convention Against Transnational Organized Crime, because they have the following elements:

1. Cross-border credit card data theft: Perpetrators can steal credit card data from various countries through online forums (Pratama, 2021).
2. Perpetrators and targets are in different countries: Perpetrators carry out hacking from one country, but the target is in another country (Alfian, 2022).
3. Collaboration with foreign parties: Carders often work with overseas colleagues who work in retail outlets to obtain customer credit card data (Putri, 2022).

4. Global access and the limitless nature of internet technology: The internet allows perpetrators to commit crimes from anywhere without having to be in the same location as the victim (Hakim, 2023).

Efforts to address carding crimes require a comprehensive approach, including:

1. Improving banking system security: Banks must improve security technologies such as multi-factor authentication and end-to-end encryption (Kusuma, 2021).
2. Increasing public awareness: Educational campaigns to improve customer understanding of cybercrime threats (Wijaya, 2022).
3. Increasing law enforcement capacity: Training for cyber investigators in handling carding cases (Hidayat, 2022).
4. Preparing stricter regulations: The government needs to revise and tighten regulations related to cybersecurity (Santoso, 2023).

Carding crime is a serious challenge in the digital world that continues to develop along with advances in information technology. With increasingly sophisticated modus operandi, both online and offline, carding perpetrators can access and misuse credit card information across countries. Law enforcement efforts require strengthening regulations and increasing security in the banking and information technology sectors. In addition, public awareness in maintaining the security of personal data is also a key factor in preventing carding crimes in the future.

Eradication of Child Exploitation Perpetrated by Law Enforcement

Barda Nawawi Arief stated that cybercrime is a new form or dimension of modern crime that has received widespread attention in the international world. Cybercrime is one of the negative impacts of technological advances that poses a serious threat to information systems, businesses, and digital finance (Arief, 2018). In the context of banking, carding crimes involving the manipulation of credit card or ATM data are becoming increasingly common, especially with increasingly sophisticated technological developments. This crime is often committed by individuals who have expertise in the field of information technology, either individually or in organized groups (Maulana, 2020).

Technology-based banking crimes have distinctive characteristics that distinguish them from conventional crimes. The modus operandi used in carding cybercrime involves various techniques such as unauthorized access, illegal contents, data forgery, cyber espionage, cyber sabotage and extortion, and infringements of privacy (Sutarman, 2019). The factors causing this crime include the development of information technology, economic motivation, weaknesses in bank security systems, and negligence of internet users in maintaining the security of personal data (Rahardjo, 2021). According to Aman Nursusila's research, the main factors influencing cybercrime in banking are the urge to test internet technology capabilities (66.6%) and economic motives (33.3%) (Nursusila, 2020).

The main obstacles in overcoming cybercrime, especially carding, are the suboptimal legal instruments, limited capacity of investigators in handling technology-based crimes, and the lack of adequate digital evidence (Hidayat, 2022). Several other obstacles faced in efforts to enforce the law on banking crimes include differences in legal interpretations related to digital evidence, lack of understanding of law enforcement officers regarding banking operations, and the rapid development of modus operandi that are difficult for cybersecurity authorities to track (Pratama, 2021). To overcome these obstacles, it is necessary to increase coordination between law enforcement agencies and modernize regulations related to cybercrime.

In order to overcome cybercrime, the UN Congress VIII/1990 concerning Computer Related Crimes proposed several policies, including modernizing criminal law, strengthening cybersecurity systems, increasing public awareness of cybercrime, and protecting victims of cybercrime (UNODC, 2020). In addition, several steps that can be taken to prevent carding crimes include the use of always updated security software, encryption of digital transaction data, periodic checks on credit card transaction history, and increasing user awareness of digital-based fraud modes (Ministry of Communication and Information, 2021).

Normatively, the formulation of cybercrime in the legal system in Indonesia still faces various challenges. Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE) has so far accommodated several aspects of cybercrime, but has not specifically regulated carding crimes comprehensively (Setiawan, 2021). Therefore, it is necessary to revise existing regulations to be more effective in overcoming digital technology-based crimes. One alternative that can be done is to integrate carding crimes into the Criminal Code as a general crime or stipulate it in special regulations as a cyber crime that has its own characteristics (Mahendra, 2022).

4. CONCLUSION

Based on the research results that have been presented in the previous chapters, it can be concluded that the main factors causing cybercrime in the form of credit card or ATM data manipulation include exploration of capabilities in the field of internet technology (66.6%) and economic factors (33.3%), which are supported by various factors such as technical aspects, socio-economic conditions, weak banking supervision systems, carelessness of internet users, and lack of network security systems and community control; in addition, the modus operandi of carding cybercrime includes Unauthorized Access to Computer System and Service, Illegal Contents, Data Forgery, Cyber Espionage, Cyber Sabotage and Extortion, Offense against Intellectual Property, and Infringements of Privacy; while in terms of law enforcement, the obstacles faced in handling carding cybercrime include weaknesses in legal instruments, limited investigator capacity, limited evidence, and lack of computer forensic facilities, so that one of the efforts made to overcome this challenge is to draft a Draft Law on Information and Electronic Transactions (RUU ITE) which includes special criminal provisions related to cybercrime, including carding crimes.

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

Anifowose, T., & Ekperiware, M. (2022). The effect of automated teller machines, point of sale terminals and online banking transactions on economic growth in Nigeria. Open Access Research Journal of Science and Technology, 4(2), 016-033.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Bhanawat, H., & Khang, A. (2024). An Examination of Data Protection and Cyber Frauds in the Financial Sector. In Data-Driven Modelling and Predictive Analytics in Business and Finance (pp. 345-360). Auerbach Publications.

Creswell, J. W. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(3), 100073.

Katarina, S. N., Boro, M., & Dragan, Ž. (2023). FORGING PAYMENT CARDS AND CYBERCRIME.

Kumar, S. (2023). CYBER CRIME: A Review. International Journal of Advanced Scientific Innovation, 5(12).

Maluleke, W. (2023). Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. International Journal of Social Science Research and Review, 6(6), 223-243.

Manaf, I. (2023). Analysis of Carding Crime as A Form of Cyber Crime in Indonesian Criminal Law. JLASA (Journal of Law and State Administration), 1(1), 1-7.

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. International Journal of Business, Economics, and Social Development, 2(4), 143-152.

Mubeen, M., Arslan, M., & Anandhi, G. (2022). Strategies to Avoid Illegal Data Access. Journal of Communication Engineering & Systems, 12(3), 29-40p.

Neuman, W. L. (2014). Social research methods: Qualitative and quantitative approaches (7th ed.). Pearson Education.

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, 163965-163986.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

Saputra, S. (2022). Analisis Pembuktian Hukum Perkara Tindak Pidana Penggelapan Melalui Elektronik Sistem (Studi Perkara Nomor 118/Pid. B/2021/Pn Cbn) (Master's thesis, Universitas Islam Sultan Agung (Indonesia).

Sinaga, H. (2023). Legal and Ethical Implications in Data Theft Cases in the Digital Era. East Asian Journal of Multidisciplinary Research, 2(11), 4585-4604.

Sogenbits, T., & Turksen, U. (2024). Cracking the Code: Unveiling Carding Crime through the Darknet-Acquired Criminal Carding Manual and the Business Model Canvas. Journal of Economic Criminology, 100071.

Stojkovic, K. N., Merdovic, B., & Zivaljevic, D. (2023). Forging Payment Cards and Cybercrime. Law Theory & Prac., 40, 138..