Analysis of Online Fraud Crimes in Buying and Selling Roblox Accounts on Social Media (Facebook) Based on The ITE Law

Safitri Handayani[1]*, Sri Pramudya Wardhani[2]

[1,2] Faculty of Law, Esa Unggul University, Jakarta, Indonesia
*Corresponding Author:
Email: safitrihdn@gmail.com

Abstract

The development of information technology and the increasing popularity of online games, particularly Roblox, have led to the emergence of the practice of buying and selling game accounts through social media such as Facebook. These transactions are generally conducted informally without adequate legal protection mechanisms, thus opening up opportunities for fraud. This study aims to analyze the types of fraud that occur in the buying and selling of Roblox accounts on Facebook and examine the criminal sanctions stipulated in "Law Number 1 of 2024 concerning Electronic Information and Transactions." Identifying the specific fraud schemes employed and evaluating the criminal penalties imposed by the ITE Law in relation to the concepts of legal protection and legal certainty are the primary concerns of this study. Using a literature review of laws, scientific publications, and other legal materials, this study follows a normative legal research methodology that draws on conceptual and statutory sources. The study findings indicate that the dominant fraud modes include social engineering, non-delivery fraud, the use of fake identities, and account reclaim, which result in material losses in the form of the loss of digital assets of economic value. In addition, the act fulfills the elements of a criminal act as regulated in "Article 28 paragraph (1), Article 30, Article 32, and Article 36 of the ITE Law". This study concludes that the ITE Law has provided a basis for legal certainty and legal protection for victims of digital transaction fraud, but it is still necessary to strengthen law enforcement and digital literacy in society.

Keywords: *Roblox Account; Online Fraud; Legal Protection; Electronic Transactions and ITE Law.*

I. INTRODUCTION

Online gaming refers to a form of video game that operates over a computer network, typically using an internet connection. Before the internet became widespread, such games could be accessed through alternative technologies such as modems or direct cable connections between computers. Over time, the growth of online gaming mirrored the rapid advancements in computer networking—evolving from local network-based games to massive global platforms as internet access expanded worldwide. The variety of online games today is vast, encompassing everything from simple text-based adventures to highly sophisticated games with immersive graphics. These modern games often feature expansive virtual environments that allow multiple players to connect, communicate, and compete with each other in real time, creating vibrant digital communities worldwide (Pratama et al., 2022).The development of online games that create dynamic digital communities has given birth to virtual communities or netizens, where interactions exceed virtual boundaries and affect real life, thus giving rise to the need for legal regulations to anticipate negative impacts such as fraud or addiction amidst increasing digital dependency (Ahmad M. Ramli, Tasya Safiranita Ramli, 2025).Along with the rapid advancement of computer network and internet technology, the development of online games has expanded interactions between players beyond the boundaries of the game itself and into the virtual world.

This phenomenon demonstrates that information technology has given rise to new patterns of life in a society increasingly dependent on the digital world. The emergence of these new activity spaces has given rise to what is known as a virtual society or netizen (internet citizen). However, internet activity does not always have positive impacts, as it also carries the potential for negative impacts. Therefore, preventative and mitigating measures are needed to minimize the negative impacts of this technological development (Badruzaman, 2019).According to a report released by Verizon, the initial phase of the 2020 lockdown showed a significant surge in mobile game downloads of 75% compared to the period before the COVID-19 outbreak (Dwi Jatmiko, 2021).Roblox is an online platform and storefront where users play games. Roblox is similar to Steam, featuring numerous games created by other developers, or simply by users themselves.

Initially, account creation is free, but within the game, users can purchase virtual items to customize their avatars, such as clothing, accessories, emojis, and more. Roblox also offers map game passes, which can be purchased using Robux to increase levels or purchase special items within the map. This can also increase the market value of a Roblox account, as users have purchased numerous items or map game passes.

However, despite its progress and popularity, there are cybersecurity threats that could potentially harm young users, particularly in the crime of buying and selling Roblox accounts. Most Roblox account sellers prefer to use social media for transactions rather than e-commerce platforms. This is evidenced by the Facebook group "Informasi Scammer JB Roblox," which provides information about fraudsters selling Roblox accounts. The group has 822 followers and over 100 posts containing screenshots detailing the perpetrators of Roblox account fraud.As for the case of fraud in buying and selling Roblox accounts on social media (Facebook) that the author found, namely the author's friend yA victim of a Roblox account fraud scam lost his account after initially purchasing it from someone else on Facebook. After a few days of use, the account was hacked by the seller, leaving him unable to log back in. He lost approximately 1 million rupiah, as the account contained numerous virtual items and Robux, which he purchased using Indonesian Rupiah.Fraud in the context of buying and selling Roblox accounts via social media is a form of cybercrime that harms consumers, both economically and psychologically. To avoid proper legal protection, perpetrators often use fake identities and conduct transactions outside of official systems.

This is why it is crucial to examine the various legal protections and law enforcement mechanisms in place to prevent such fraudulent acts. Based on "Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions," those who intentionally spread false or misleading information that causes consumer losses in electronic transactions can be subject to criminal penalties, as stated in Article 28 paragraph (1) of the ITE Law, along with related sanctions. Fraudulent buying and selling of online game accounts such as Roblox contains elements of criminal fraud as stated in "Article 492 of the Criminal Code (KUHP) and can be prosecuted under the ITE Law. However, many obstacles remain in handling this case, including law enforcement's limited understanding of digital aspects and challenges in tracing perpetrators who use fictitious identities on social media.Based on the explanation above, the researcher believes it is necessary to conduct a study on fraudulent activities in the buying and selling of Roblox accounts on Facebook, based on the ITE Law. It is hoped that this research will contribute to legal knowledge and provide useful recommendations for strengthening legal protection for consumers in digital transactions and strengthening law enforcement against online fraudulent practices.

II. METHODS

This research follows the standards of normative (doctrinal) legal theory by analyzing key legal concepts and conducting an extensive literature review. (Dr. H. Nur Solikin, S.Ag., 2021). Both statutory and conceptual approaches are used in conducting this normative legal research. In implementing a legislative strategy, the author must first investigate relevant laws and regulations related to the research subject. As stated by Ibrahim in Theory and Methodology of Normative Legal Research, standards of behavior mandated by law are the primary subject of normative legal research. Therefore, the analysis in this study focuses on "Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 1 of 2024," along with implementing regulations and other relevant legal provisions, to assess their suitability and applicability to the issue of fraud in electronic transactions. (Herrenauw et al., 2022) This research utilizes various primary, secondary, and tertiary legal sources. Law Number 1 of 2024 concerning Electronic Information and Transactions, its implementing regulations, and other laws and regulations related to electronic transactions and criminal fraud constitute the primary sources of legal literature. Books, scientific journals, articles, findings from previous research, and expert commentaries on the topic of internet fraud are examples of secondary legal documents that can enhance the analysis and provide a more comprehensive academic perspective on the topic.

The legal terms used in this investigation are sourced from tertiary legal literature such as dictionaries and encyclopedias.By searching for and collecting various laws, legal instruments, and academic sources related to the research subject, legal materials were collected through a literature review. Next, a

logical analysis procedure was applied to methodically examine all collected legal data. The analysis stage began with editing, which involved examining and refining the legal materials to ensure they were complete and formulated in clear language. Next, systematization was carried out, which involved grouping and classifying the legal materials according to their type and logical relevance. The final stage was description, which involved presenting and analyzing the research results based on the legal materials obtained. An in-depth interpretation of the provisions of laws and regulations related to the research problem constitutes the qualitative data analysis approach used in this study. Subsequent analysis focused on assessing the suitability of applicable positive legal norms with the fraudulent practice of buying and selling Roblox accounts on Facebook. Based on the results of this interpretation and analysis, the researcher systematically developed legal arguments to draw conclusions regarding the fraudulent methods and the criminal provisions applicable to the perpetrators. Therefore, this analysis is expected to provide a comprehensive and structured understanding of online fraud in Roblox account buying and selling transactions.

III. RESULT AND DISCUSSION

Types of Fraud That Occur in Buying and Selling Roblox Accounts on Social Media

The types of fraudulent practices occurring in the buying and selling of Roblox accounts on social media demonstrate a shift from conventional fraudulent practices to the digital space, as community-based online transactions increase. One dominant method is social engineering, a psychological manipulation technique that exploits victims' trust, haste, and lack of digital literacy to gain unlawful profits. Social media platforms like Facebook, which lack escrow mechanisms or transaction protection, provide an ideal platform for perpetrators to carry out this practice. This situation demonstrates that fraudulent practices in the buying and selling of online game accounts are not merely individual but have become a systemic pattern of cybercrime. Therefore, it is crucial to examine this phenomenon from the perspective of cyber law and consumer protection to understand the urgency of adaptive regulations to the development of digital transactions. (Dr. Iman Sjahputra, SH, Sp.N., 2021). This phenomenon can be clearly observed through the Facebook group "Informasi Scammer JB Roblox," which serves as a platform for sharing victim reports of Roblox account buying and selling scams. In this group, many members post reports of non-delivery fraud, where the perpetrator offers accounts with high specifications, such as Robux and rare items, but after payment is made, the account is never delivered or the victim is immediately blocked by the perpetrator. (Farizy, 2024) In addition to non-delivery fraud, reports in the group also indicate a fake profile scam, where perpetrators use fake or hacked Facebook accounts to conduct transactions.

The use of these fake digital identities aims to avoid legal liability in the event of a dispute. (Vebri et al., 2025) Another frequently occurring method relevant to the cases studied by the author is account reclaiming or hackback. In this method, the perpetrator sells a Roblox account to the victim, but after some time using the account, the victim loses access because the perpetrator exploits the account recovery data or initial access to illegally reclaim the account. This pattern is also frequently reported in the "JB Roblox Scammer Information" group, particularly for accounts that initially appear safe and can be used for several days before being reclaimed. (I Gusti Made Darwin Damareksa Putra & Dewa Gede Pradnya Yustiawan, 2024) The specific case experienced by the victim in this study follows a pattern identical to the reports in the group. The victim purchased a Roblox account through Facebook for approximately IDR 1,000,000.00 based on virtual items and Robux purchased using Indonesian Rupiah. After several days of transactions and account use, the perpetrator hacked the account, resulting in the victim losing access to it and all digital assets. This confirms that the account reclaim scheme is a systemic and recurring form of fraud, not a single incident.From a cybercrime law perspective, this act fulfills the elements of electronic fraud as stipulated in "Law Number 1 of 2024 concerning Electronic Information and Transactions.

" The element of fraud is fulfilled through the deception of selling the account, the element of unauthorized access is fulfilled through the takeover of the account, and the element of actual loss arises from the loss of digital assets of economic value. (Mubarak, 2023).Thus, the reports documented in the Facebook group "JB Roblox Scammer Information" reinforce the analysis that the fraudulent method of buying and selling Roblox accounts on social media is systemic, repetitive, and exploits weaknesses in

informal transactions. The existence of this community not only serves as a warning to users but also serves as concrete evidence of a cybercrime pattern that demands strict and adaptive legal enforcement in response to the development of digital assets.Based on the discussion of the fraudulent case of buying and selling Roblox accounts via Facebook, the main problem lies not only in the perpetrators' actions, but also in the weak legal protection for informal digital asset transactions. The lack of specific regulations regarding the buying and selling of online game accounts creates a legal loophole that perpetrators often exploit to commit fraud in bad faith.In the context of national cyber law, fraudulent practices in the buying and selling of Roblox accounts underscore the need for specific regulations governing digital asset transactions. These regulations should cover ownership, transfer procedures, and legal protection mechanisms against potential disputes. Without clear provisions, victims will remain vulnerable due to the difficulty of proving ownership of accounts and virtual items in the legal realm. Therefore, the establishment of legal norms responsive to developments in information technology is urgently needed to close legal loopholes exploited by fraudsters (Ummah, 2019).

Criminal Sanctions in Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law) Regulate Criminal Acts of Fraud Related to the Buying and Selling of Roblox Accounts on Social Media (Facebook)

"Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law) is a national legal umbrella that revises and strengthens criminal provisions for unlawful acts committed through electronic systems, including fraud in digital transactions." This update is important from a legal certainty perspective because it provides a clearer definition and strict sanctions for perpetrators of electronic-based fraud so that there is no multiple interpretations in law enforcement. 1 In addition, the ITE Law also functions as a legal protection instrument for consumers in the digital realm, ensuring that losses due to electronic transaction fraud receive equal legal treatment as conventional fraud (Pakina, 2023).The ITE Law not only provides a comprehensive legal framework to address the misuse of electronic systems, but also bridges general provisions with concrete cases such as digital fraud on social media platforms, thus enabling adaptive and responsive law enforcement to the dynamics of online transactions (Dr. Danrivanto Budhijanto, SH, 2025).In the case of the Roblox account fraud perpetrated through Facebook, the perpetrator sold the account to the victim and then took it back through hacking, resulting in the victim losing access even after making a payment of Rp1,000,000.00. This act constitutes a form of fraud involving the unauthorized use of an electronic system and causing real harm, making it relevant to criminal sanctions under the ITE Law.

First, Article 28 paragraph (1) of the ITE Law states that “any person who intentionally and without the right to disseminate electronic information and/or electronic documents containing false notifications or misleading information that results in consumer losses in electronic transactions” shall be punished (Mustikajati et al., 2024). The element of intentionally and without rights is fulfilled because the perpetrator knowingly offers an account and accepts payment in bad faith; the element of misleading electronic information is fulfilled because the perpetrator provides a description of the account owned when in fact it is still under his control; and the element of consumer loss is clearly visible from the loss of digital assets of economic value. Article 28 paragraph (1) is a manifestation of legal certainty regarding digital fraud, where the ITE Law expands the scope of fraud crimes from general crimes in the Criminal Code to the realm of electronic transactions. Second, Article 45A paragraph (1) of the ITE Law “regulates criminal sanctions for violators of the provisions of Article 28 paragraph (1), namely a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah)”. This sanction provides legal certainty in the form of a clear criminal threat, as well as a preventive function for perpetrators who might be tempted to commit similar fraud in the future.

Third, a relevant but often complementary norm is the prohibition on unauthorized access to electronic systems, as stipulated in Article 30 of the ITE Law, which ensnares perpetrators who hack or take over accounts after a transaction is completed (Joint Decree of the Minister of Communication and Information of the Republic of Indonesia and the Attorney General of the Republic of Indonesia, 2021). The fact that an account that has been paid for is then repossessed indicates a violation of the victim's right of access to their electronic information. Fourth, Article 32 of the ITE Law emphasizes the prohibition on

unauthorized taking over, transferring, or controlling another person's electronic information, which in the context of this case is a Roblox account and virtual items of economic value. The transfer of control of the account from the victim back to the perpetrator fulfills the elements of this article. Fifth, Article 36 of the ITE Law requires that losses occur as a result of these actions, impacting the victim's legal rights and interests. These losses are not only material, but also the loss of digital assets, which are increasingly recognized as a form of wealth in the digital economy and worthy of legal protection.

The principle of lex specialis derogat legi generalis confirms that the ITE Law is more appropriate than Article 492 of the Criminal Code. The application of the ITE Law as lex specialis provides legal certainty relevant to the reality of modern digital transactions (Ibrahim, 2016). The criminal sanctions stipulated in the ITE Law are not only repressive in nature to punish perpetrators, but also preventive in nature to provide a deterrent effect to the public. The application of strict sanctions against perpetrators of online fraud will encourage the public to be more careful in conducting digital transactions, while strengthening public trust in electronic-based transactions. Previous studies have shown that the implementation of criminal sanctions in the ITE Law against online fraud has been running according to the legal mechanisms in the police in handling online fraud cases, although still encountering practical obstacles in the field.On the other hand, electronic system administrators, both social media platforms and online game operators, need to play an active role in strengthening account security systems and preventing account reclaim practices. Strengthening account ownership verification and restricting account recovery by the previous owner after a transaction can be crucial steps to reduce the potential for fraud (Pratama et al., 2022).

Therefore, addressing Roblox account fraud requires a multi-layered strategy that includes stricter enforcement of the Electronic Information and Transactions Law, increased education on digital law, and revised policies to accommodate changes in how digital assets are transacted. The goal of this initiative is to strengthen victim protection laws and make online purchases safer (Amalia et al., 2024).

IV. CONCLUSION

Based on the discussion, it can be concluded that fraudulent practices in buying and selling Roblox accounts on Facebook are developing systematically and repeatedly along with the increase in informal digital asset transactions. The most dominant methods include social engineering, non-delivery fraud, the use of fake identities, and account reclaim, which is the takeover of an account by the seller after the transaction is completed. These methods exploit the weak transaction protection system on social media and the low level of digital legal literacy in the community. The existence of the Facebook group "Informasi Scammer JB Roblox" reinforces the finding that this fraudulent practice is not an incidental event, but rather a widespread and organized phenomenon, with a relatively uniform pattern. Roblox accounts and the virtual items and Robux contained within them have real economic value, so losing access to these accounts results in significant material losses for victims. Therefore, fraudulent practices in buying and selling Roblox accounts can be classified as a form of cybercrime that requires serious legal action and adapts to developments in the digital economy.

The criminal sanctions provisions in “Law Number 1 of 2024 concerning Electronic Information and Transactions have provided a clear and firm legal basis to ensnare perpetrators of fraudulent buying and selling of Roblox accounts on Facebook social media”. The perpetrators' actions in the case under study fulfill the elements of electronic-based fraud, unauthorized access, unauthorized control of electronic information, and causing losses as stipulated in “Article 28 paragraph (1), Article 30, Article 32, and Article 36 of the ITE Law, with the threat of criminal sanctions stipulated in Article 45A”. The application of the ITE Law as lex specialis provides more relevant legal certainty than conventional fraud provisions in the Criminal Code, while strengthening legal protection for victims of digital transactions. Therefore, the ITE Law has a dual purpose: to punish perpetrators of violations through action, and to prevent future violations by creating a safe, fair, and clear legal climate in the era of digital assets.

V. SUGGESTION

Based on the results of this study, it is recommended that the government and policymakers develop more specific regulations regarding digital asset transactions, including the buying and selling of online game accounts, to provide legal certainty regarding account ownership and transfers and close legal loopholes that have been exploited by fraudsters. Law enforcement officials need to improve their capacity and technical understanding of cybercrime so that enforcement of Law Number 1 of 2024 concerning Electronic Information and Transactions can be implemented effectively and consistently.

Electronic system operators, both social media platforms and online game operators, are expected to strengthen their security systems and account ownership verification to prevent account reclaim practices. Furthermore, improving legal literacy and digital literacy among the public is crucial to encourage users to be more cautious in conducting electronic transactions. Future researchers are advised to develop studies using an empirical or comparative approach to assess the effectiveness of the implementation of the ITE Law and expand analysis of the legal protection of digital assets in online transactions in Indonesia. Furthermore, future researchers are advised to develop normative legal research by expanding conceptual studies and comparing national and international laws and regulations to enrich future analysis of legal protection for digital assets and cybercrime.

REFERENCES

[1] Amalia, EY, Isnawati, M., & Protection, L. (2024). Legal protection for victims of fraudulent sales transactions on the marketplace.

[2] Budhijanto, D. (2025). Cybercrime law 4.0: Digital crime and artificial intelligence (AI). Gramedia.

[3] Farizy, SA (2024). Legal protection for consumers in cases of e-commerce transaction fraud.

[4] Herrenauw, JM, Alfaromona, J., Titahelu, S., & Saimima, JM (2022). A criminal law study of fraudulent online game account sales through social media. ***Journal***, 2(3), 252–261.

[5] Joint Decree of the Minister of Communication and Informatics of the Republic of Indonesia, the Attorney General of the Republic of Indonesia, and the Chief of the Indonesian National Police. (2021). Joint Decree Number 229 of 2021, Number 154 of 2021, Number KB/2/VI/2021 (pp. 1–22).

[6] Mubarak. (2023). Factors related to handling criminal acts. Journal, 1(1), 19–24.

[7] Mustikajati, AA, Jalan, A., Sutami, I., & Tengah, J. (2024). Fraud as another person's property as regulated in Article 378 of ***the Criminal Code. Journal***, 1(2).

[8] Pakina, R. (2023). Electronic Information and Transactions Law and business development in Indonesia: Confrontational or accommodative? Commitment: ***Management Scientific Journal***, 4(1), 234–242.

[9] Pratama, RM, Widyasari, W., & Nisa, DA (2022). Fraud prevention in online game buying and selling transactions using animation media. ***Jurnal Imajinasi***, 6(1), 46. https://doi.org/10.26858/i.v6i1.32861

[10] Ramli, AM, Ramli, TS, & C., FG (2025). Telematics Law (3rd Edition). Open University.

[11] Solikin, N. (2021). Introduction to legal research methodology. https://digilib.uinkhas.ac.id/12273/

[12] Sjahputra, I. (2021). Consumer protection in electronic transactions: Reviewed from the perspective of consumer protection law and cyber law.

[13] Ummah, MS (2019). Introduction to cyber law.

[14] Vebri, T., Setiawan, A., & Khairunissa, A. (2025). ***Personal data protection in AI technology: Analysis of the role of law and regulatory compliance in digital business. Journal***, 14(2), 191–207.