HERMENEUTIKA
VOL. 10, NO.2, AUGUST 2026
p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

CRIMINAL LAW STUDY ON ONLINE FRAUD MODE THROUGH WHATSAPP APPLICATION

Anisa Fitriani[1], Endang Sutrisno[2], Dadan Taufik F[3]

[123] Universitas Swadaya Gunung Jati, Indonesia

DOI: https://doi.org/10.33603/hermeneutika.v10i2.11837
Accepted: 01 April 2026 ; Revised: 30 Juli 2026; Published: 02 August 2020

Abstract: *The rapid advancement of information and communication technology has significantly influenced people's daily lives, particularly in terms of financial transactions and social interactions conducted through electronic media. However, this progress has also created new opportunities for criminal activities, one of the most prominent being online fraud. The incidence of online fraud continues to rise, with increasingly varied modus operandi that exploit social media platforms and instant messaging applications, resulting in financial losses for the public and posing challenges for law enforcement authorities. This study aims to identify the various forms of online fraud schemes in Cirebon City and to examine the legal frameworks applied by law enforcement agencies in addressing such crimes. The research adopts a normative juridical approach, incorporating statutory, conceptual, and case-based analyses. It is primarily a normative legal study supported by limited empirical data, utilizing primary, secondary, and tertiary legal sources that are analyzed qualitatively. The findings reveal that online fraud in Cirebon City manifests in several forms, including fraudulent online transactions, investment scams, online rotating savings (arisan), and impersonation of institutions or trusted parties. These schemes generally rely on exploiting victims' trust through digital communication channels. In practice, law enforcement officers predominantly rely on Article 378 of the Criminal Code due to its practicality and relative ease in evidentiary procedures. Meanwhile, the application of the updated 2024 Electronic Information and Transactions Law still encounters obstacles, particularly in proving specific legal elements that often require expert testimony. Consequently, enforcement efforts tend to combine conventional criminal law with selective application of cyber law. The study concludes that strengthening regulations, enhancing the capacity of law enforcement personnel, and increasing public legal awareness are essential to ensure more effective and equitable prevention and enforcement against online fraud.*

Keywords: Online Fraud, Criminal Offenses, Law Enforcement, Modus Operandi, Cirebon City.

I. INTRODUCTION

Along with the development of the needs of the global community, information technology has an important impact on changes in the present and future. Because these developments have many advantages and positive impacts for countries in the world. There are at least two things that make information technology considered so important in spurring the growth of a country in the world. First, information technology makes an increase in demand for information technology products themselves, such as computers, modems, smartphones, laptops and so on.

Second, it is to facilitate the activities of the global community, one of which is in terms of communication.

In this century, almost all human activities are carried out with the help of information and communication technology. Starting from activities in the economic, social, transportation, to defense sectors, it is very dependent on the internet. The century is known as a new era, namely the 4.0 era or the digital economy era.

The development of technology and information today has changed the way people from all walks of life socialize from what was initially conventional to online. The development of technology and communication that makes it easier for the public to absorb and share information with individuals and the public. The rapid advancement of technology and internet development makes anyone can access, have a network and easily disseminate more massive information because there are no restrictions on place and time in the internet world. The internet provides a social variety that is much different from real life. This is then called cyber.

The development of information technology on the one hand brings positive things but on the other hand also brings negative things to society. The positive impact is to provide a lot of convenience for humans in carrying out their activities. Meanwhile, one of the negative impacts is making it easier for people to commit crimes in cyberspace, which is often known as *cyber crime*. Cyber crime or cybercrime is an act of crime that takes advantage of the development of computer technology. Cybercrime itself is an unlawful act that utilizes computer technology based on the sophistication of the development of internet technology which is carried out by using computer networks as means/tools or computers as objects, whether to gain profit or not, by harming other parties.

One of them is the increasing use of instant messaging applications, especially WhatsApp, which is now the main means of communicating, transacting, and carrying out social and economic activities. WhatsApp itself is the most used application in Indonesia not only because of its easy use, but also for several other reasons. One of them is the factor of a very large number of users, so almost everyone can easily communicate without the need to ask what application they are using. This condition creates a network effect, where the more people who use WhatsApp, the more obligatory it is for other people to use it.

However, behind the benefits, there is also a negative side in the form of rampant *cybercrime*. And one of the most common *cyber crimes* is online fraud. The mode of fraud through WhatsApp is often carried out in various ways, such as perpetrators who disguise themselves as relatives or friends and some on behalf of the expedition. There is even a mode of arisan fraud carried out through the WhatssApp application which is detrimental to many victims. This mode takes advantage of public trust and weak digital literacy so that many victims are harmed, both materially and psychologically.

Juridically, the crime of fraud has been regulated in the Criminal Code (KUHP), especially Article 378 which regulates conventional fraud. However, with the development of information technology, a special arrangement was born in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, which provide a firmer legal basis for criminal acts committed through electronic means. However, there are still problems in the application of the law, both related to proof, jurisdiction, and the effectiveness of law enforcement against perpetrators who are often difficult to track because they use false identities.

This condition creates urgency to conduct a more in-depth juridical study on the mode of online fraud through WhatsApp. This analysis is needed to understand the extent to which criminal law instruments, both contained in the Criminal Code and the ITE Law, are able to provide

legal protection for the community and provide legal certainty in the enforcement of justice. In addition, this research is expected to make an academic and practical contribution in formulating strategies to counter fraud crimes based on information technology, which are increasingly complex.

II. RESEARCH METHODS

The research method in this study aims to analyze law enforcement against online fraud through the WhatsApp application from a criminal law perspective. This research uses a normative juridical approach with a descriptive-qualitative method to understand how the applicable criminal law provisions, both in the Criminal Code and the Electronic Information and Transaction Law (UU ITE), are applied in the face of increasingly complex modes of online fraud.

The juridical approach is used to examine various relevant laws and regulations, such as Article 378 of the Criminal Code and Article 28 paragraph (1) jo. Article 45A paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. This analysis is complemented by the doctrine of criminal law experts and law enforcement theories put forward by Soerjono Soekanto. Thus, this study not only focuses on normative aspects in the form of written legal rules, but also highlights obstacles that arise in law enforcement practices, such as the difficulty of digital proof, tracking the identity of perpetrators, and low digital literacy of the community.

1. Types and Sources of Legal Materials

The type of legal material used in this study is qualitative data obtained through literature studies. The data source consists of:

1) Primary Legal Materials, namely laws and regulations that are the legal basis for online fraud, include Article 378 of the Criminal Code, Article 28 paragraph (1) jo. Article 45A paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as other relevant laws and regulations.
2) Secondary Legal Materials, in the form of doctrines, books, journals, scientific articles, previous research results, as well as the opinions of criminal law and cyber law experts related to the problem of online fraud.
3) Tertiary Legal Materials, which are supporting materials that provide additional understanding, such as legal dictionaries, encyclopedias, and official online sources that can help explain legal terms and concepts used in research.

2. Legal Materials Collection Techniques

The technique of collecting legal materials in this study is carried out through two main methods, namely literature studies and limited interviews, in order to obtain comprehensive and in-depth data.

1) Literature Studies
   Literature studies are carried out by tracing, reviewing, and analyzing primary, secondary, and tertiary legal materials that are relevant to research problems. Primary legal materials are in the form of laws and regulations such as Article 378 of the Criminal Code and Article 28 paragraph (1) jo. Article 45A paragraph (1) of Law Number 19 of 2016 concerning ITE. Secondary legal materials are books, journals, articles, and previous research that discusses online fraud and cybercrime. Meanwhile, tertiary legal materials in the form of legal dictionaries, encyclopedias, and official online sources are used to clarify legal terms.
2) Limited Interviews
   Interviews were conducted on a limited basis with law enforcement officials, such as investigators at the Directorate of Cyber Crime of the National Police Criminal

Investigation Branch or Kominfo officials who handle public complaints. The purpose of this interview was to obtain additional information about the obstacles and challenges in law enforcement against online fraud through WhatsApp. Data from interviews are complementary and are not the primary source of research.

3. Legal Materials Analysis Techniques

The legal materials obtained in this study are analyzed using normative qualitative analysis methods, namely analysis that emphasizes the interpretation of relevant laws and regulations, doctrines, and legal theories. This analysis aims to explain the content of legal norms, relate them to the problem of online fraud, and assess the effectiveness of the application of criminal law in practice.

1) Reduction of Legal Substances
   Legal materials obtained from primary, secondary, and tertiary legal materials were selected to determine information relevant to the focus of the research, namely the crime of online fraud through the WhatsApp application.
2) Presentation of Legal Materials
   The reduced legal materials are then systematically compiled in the form of narrative descriptions, with reference to the established research structure.
3) Conclusion Drawdown
   The legal materials that have been analyzed are linked to Soerjono Soekanto's law enforcement theory, so that conclusions are drawn about the extent to which the provisions of the Criminal Code and the ITE Law are effective in dealing with online fraud modes.

4. Legal Materials Testing Techniques

In order for the legal materials obtained in this study to have a high level of validity and reliability, the triangulation method is used as a technique for testing legal materials. Triangulation is a process of cross-examining data obtained through various sources, methods, and theories, so that research results can be more objective, accurate, and reliable. This technique is important to avoid bias in research as well as ensure that the legal materials used accurately reflect the realities that occur in law enforcement practice. The triangulation technique used in this study consists of three types, namely:

1) Tringulation Source
   Source tringulation is carried out by comparing and confirming data obtained from various legal sources and sources. In the context of this research, data from laws and regulations (Criminal Code and ITE Law), academic literature, and official reports from the National Police and Communication and Informatics will be compared to ensure the correctness and consistency of information. If there are differences in data, this study will further explore the causes of these differences to obtain more accurate conclusions.
2) Tringulation Theory
   Theory tringulation is carried out by analyzing data using various legal theory perspectives to obtain more comprehensive conclusions. In this study, the theories used include Law Enforcement Theory (Soerjono Soekanto), criminal law theory about criminal responsibility, and theories about *cyber crime*. By comparing the findings of the research against various relevant theories, this study can provide a more in-depth analysis of the effectiveness of criminal law in dealing with online fraud modes.
3) Tringulation Method

The method was tringulated by comparing the data from the literature study with the data from limited interviews with law enforcement officials. Thus, the research not only relies on normative analysis, but also receives confirmation from the reality in the field. This strengthens the validity of the data and adds to the reliability of the study's conclusions.

5. Knot Pulling Technique

The technique of drawing conclusions in this study uses a combination of deductive approaches, namely a thought process that departs from general legal norms to special (deductive) cases. This approach was chosen because the research focuses on the analysis of legal norms in Article 378 of the Criminal Code and Article 28 paragraph (1) jo. Article 45A paragraph (1) of Law Number 19 of 2016 concerning ITE, and is complemented by observations of real cases of online fraud through WhatsApp that are reported by the mass media and experienced by the public.

The stages in this conclusion drawing technique include:

1) Gradual Analysis of Legal Materials

Conclusions are drawn through the process of collecting, reducing, and presenting data. Legal materials gathered from laws and regulations, legal literature, credible news, and experiences of victims of online fraud are reduced to sort out the most relevant information. Thus, the research gained a more targeted understanding of the legal arrangements and constraints in law enforcement against online fraud.

2) Linking Research Findings to Theory and Regulation

The legal materials that have been analyzed are then compared with legal theories, especially Soerjono Soekanto's Law Enforcement Theory, as well as the applicable legal norms, namely the Criminal Code and the ITE Law. In this way, research can assess the extent to which the application of criminal law is in accordance with the objectives of community protection and whether there is a gap between normative provisions and practice in the field.

3) Preparation of Legal Recommendations

Based on the results of the analysis, this study compiles recommendations aimed at law enforcement officials, policy makers, and the public. These recommendations include concrete steps to increase the effectiveness of criminal law enforcement against online fraud through WhatsApp, including improving people's digital literacy, strengthening technical regulations, and optimizing inter-agency cooperation.

III. RESEARCH RESULTS

1. Legal Basis in Handling Online Fraud Crimes

Law enforcement against online fraud uses a combination of conventional law and electronic law, namely Article 378 of the Criminal Code and ITE Law No. 1 of 2024 (the second amendment to the 2008 ITE Law). This shows that even though crimes occur digitally, national law still refers to the elements of deception and losses regulated in the Criminal Code, while the ITE Law regulates aspects of the use of digital technology.

a. Conventional Legal Basis; Article 378 of the Criminal Code is the main basis for ensnaring perpetrators of online fraud. This article states: "Whoever who, with the intention to unlawfully benefit himself or others, by means of deception, forces a person to hand over goods, money, or securities, shall be punished with imprisonment for a maximum of four years." [3] Some important points of this article that are relevant to online fraud: Elements of deception: The perpetrator uses a fake

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

message, fictitious link or website, or false identity to deceive the victim. Element of loss: The victim is harmed materially or non-materially. Purpose of benefiting oneself or another party: The perpetrator takes financial advantage through online transactions. In addition to Article 378, Article 372 of the Criminal Code regarding embezzlement can also be used if the perpetrator controls the victim's funds or assets through an online system. Thus, the Criminal Code remains the main legal foundation, even though fraud is carried out with digital media.

b. Special Legal Basis; ITE Law No. 1 of 2024 ITE Law 2024 (the second amendment to the 2008 ITE Law) provides a special legal basis related to criminal acts that utilize information technology. Some articles relevant to online fraud include: Article 28 paragraph (1) of the 2024 ITE Law prohibits the dissemination of electronic information that is misleading and detrimental to other parties. This article ensnares perpetrators who spread fake links, fictitious lotteries, or fake investment offers. Articles 32-35 of the 2024 ITE Law regulate electronic data forgery, account manipulation, and misuse of digital identities. Perpetrators who use WhatsApp numbers or fake accounts to deceive victims can be charged with these articles. Articles 44–45 of the 2024 ITE Law Explain the collection and use of electronic evidence in the investigation and trial process. Evidence such as WhatsApp chats, transfer screenshots, or recordings of online transactions is recognized as legitimate evidence. The ITE Law provides a legal basis for law enforcement officials to take effective action against perpetrators, even if their actions occur in the digital realm. With this law, online fraud cases are no longer solely handled with conventional law, but also electronic laws that strengthen digital evidence.

c. Law Enforcement Process at the Cirebon City Police In practice, the handling of online fraud cases in Cirebon City through the Cirebon City Police involves several legal stages: Reporting Victims who feel aggrieved report incidents to the Cirebon City Police, either directly to the police station, Cyber Crime unit, or the National Police e-report. The report comes with digital evidence, such as WhatsApp screenshots, proof of transfers, or fake website links. Preliminary Investigation Officers conduct a review of reports, examine evidence, and determine whether the case is a criminal act of online fraud. This stage ensures that the report is worthy of follow-up to the investigation process. Evidence Collection Evidence consists of digital documents, witness statements, and experts, including IT experts and criminal experts. Electronic evidence is validated and determined through the District Court so that it has legal force. Phase One: Delegation of Files to the Prosecutor's Office After the administration of the investigation and the complete file, the investigator submits the file to the prosecutor's office. The Public Prosecutor (JPU) conducted a file investigation, and if complete, issued a P-21 (the file was declared complete). Stage Two: Handover of Suspects and Evidence Investigators present suspects and evidence to the JPU. After this stage, the investigator's task is completed, and the next authority lies with the prosecutor for prosecution planning.

d. Legal Obstacles in Handling Online Fraud In the practice of investigation, there are several obstacles faced by police officers; Fake WhatsApp number or SIM card Perpetrators often use registration numbers belonging to other people so that they are difficult to track. Bank accounts in the name of a third party Money transfers

are carried out through accounts belonging to other people, so investigators cannot immediately find out the identity of the account owner because it is limited by customer privacy, except for terrorism or TPPU cases. Complexity of electronic evidence Digital evidence such as screenshots or chats must be validated to be valid in court. This requires specialized expertise and rigorous digital forensic procedures. This constraint shows that even though the legal basis is complete, technical factors and privacy regulations remain challenges in law enforcement against online fraud.

e. The Cirebon City Police Community Prevention and Education Efforts also take preventive steps, including; Socialization through online media Education is carried out through official platforms such as Instagram, Facebook, Twitter, to inform the latest fraud modes and how to protect themselves. Direct education to schools and campuses This activity aims to increase digital literacy, especially related to the security of online transactions and the wise use of social media. Wise appeal to use social media The public is urged to: It is not easy to respond to unknown WhatsApp numbers. Verify information through family or people who understand technology better. Do not consume information privately without confirmation. This effort is important to reduce the risk of online fraud while increasing public awareness of digital dangers.

f. Legal Analysis and Practice Combination of Conventional and Digital Law of the Criminal Code is still used to ensnare elements of deception and loss, while the ITE Law emphasizes aspects of the use of technology and electronic evidence. The Power of Electronic Evidence Evidence of chats, links, and transfers are key in legal proceedings. The ITE Law ensures that this evidence is valid and can be processed in court. The limitations of law enforcement The privacy of banks and the use of fake numbers make the identification of perpetrators require coordination across agencies and a considerable amount of time. The role of Prevention Education through digital literacy is an important part so that potential victims can recognize the mode of fraud before losses occur.

2. The Form of Modus Operandi of Online Fraud Crimes in Cirebon City

Online Fraud Modus Operandi in Cirebon City Based on the documentation of the Cirebon City Police case and interviews with investigators, there are several dominant modus operandi that occur in this area:

a. Fake Prize Offers or Sweepstakes The perpetrator sends a message via WhatsApp or other digital media informing them that the victim has won a large prize from a well-known company, bank, or marketplace. The victim was asked to transfer administrative fees or taxes, as well as provide personal data such as account numbers and ID cards. Case in point: In 2023, a Cirebon resident received a message winning an electronic lottery worth tens of millions of rupiah. After the victim transferred an administrative fee of Rp 2,500,000, the perpetrator blocked the victim's contact. Psychological analysis shows that victims are easily tempted by the promise of large rewards without risk, so the verification process is rarely carried out.

b. Scams Under the Guise of Online Investments and Fake Trading Perpetrators offer investments through the WhatsApp application, Telegram groups, or fake trading platforms with the promise of high profits in a short period of time. The victim was directed to transfer a sum of money. Perpetrators sometimes give small initial profits as bait (trust building). After the number of members

increased, the perpetrators fled with all the funds. This kind of case often targets people who do not understand digital investment and rely on instant profits. The Cirebon City Police have handled several similar cases involving hundreds of victims.

c. Selling Fictitious Goods on Social Media Perpetrators create fake accounts on platforms such as Facebook Marketplace, Instagram, and WhatsApp to offer electronics, fashion, or vehicles at low prices. After the victim transfers the money, the goods are not sent. The perpetrator blocks the account or deactivates the WhatsApp number. This mode emphasizes the use of e-commerce and social media as a means of deception. The case was very detrimental to the victim because the promised goods were never received.

d. Bodong Online Arisan One of the modes that most often appears in Cirebon is online arisan via WhatsApp. The perpetrator created a social gathering group and recruited new members. Some of the early members were given arisan funds as "bait". After the number of members increased, the perpetrators fled with all the funds. This case shows a combination of traditional deception and modern technology, where all social gathering activities take place digitally.

e. Social Engineering (Phishing / Vishing) The perpetrator impersonates authorities, banks, couriers, or other authorized agencies to request the victim's personal information, such as OTP, PIN, or bank account password. These modes include the categories of phishing and vishing, where the victim's trust is fully exploited. The process is very fast and difficult to detect because it uses fake digital identities. This crime emphasizes the importance of digital literacy and public awareness of suspicious communications.

f. Fake Transfer Proof The perpetrator uses a forged digital transfer proof to convince the victim that the payment has been made. After the victim handed over the goods or transferred money, the perpetrator disappeared. This technique combines the forgery of digital documents with the psychology of the victim who believes in visual evidence. Digital evidence, such as screenshots or chat recordings, is key in the investigation of this case.

IV. CONCLUSION

Based on the results of the research on the Criminal Law Study on the Online Fraud Mode through the WhatsApp Application in Cirebon City, as well as the analysis of theories, positive legal provisions, and empirical findings, the following conclusions can be drawn:

Law enforcement against online fraud through the WhatsApp application in Cirebon City has a sufficient legal basis through Article 378 of the Criminal Code and Article 28 paragraph (1) jo. Article 45A paragraph (1) of the ITE Law and is strengthened by Police Regulation Number 6 of 2019 concerning Criminal Investigation. However, the effectiveness of the implementation of these regulations is still not optimal. Some of the factors that affect the weakness of law enforcement include: the difficulty of proving digital evidence, the use of fictitious identities and accounts, weak cooperation across institutions and digital platforms, and not all law enforcement officials have digital forensic technical competence. In addition, there are still dark numbers (latent numbers) due to victims being reluctant to report because they are embarrassed, afraid, or consider losses to be small. This condition shows that law enforcement

has not fully run according to the purpose of criminal law, which is to provide legal protection, legal certainty, and a deterrent effect for perpetrators.

The modus operandi of online fraud through the WhatsApp application in Cirebon City shows the development of increasingly varied, systematic crime patterns, and takes advantage of psychological weaknesses and low digital literacy of the community. The modes used by the perpetrators include identity spoofing, social gathering and fraudulent investment fraud, sending phishing links to take personal data, fraud under the guise of prizes or promos, and misuse of false information to obtain financial benefits from victims. The spread of this mode shows that perpetrators take advantage of public trust in access to quick application-based communication, as well as the lack of information verification mechanisms in the digital space. In addition, the increasing number of case reports from year to year shows that cybercrime is not just an individual act, but has evolved into an organized crime pattern and is adaptive to technological change.

BIBLIOGRAPHY

Adimi Chazawi., *"Criminal Lesson II"* of the King of Grafindo. Jakarta, 2001, pp. 67 and 69.

Agus Rahardjo, *Cybercrime-Understanding and Efforts to Prevent Technological Crimes*, Citra Aditya Bakti, Bandung, 2002, p. 1.

Eddy O.S. Hiariej, *Theory and the Law of Proof*, (Yogyakarta: Cahaya Atma Pustaka, 2019), p. 212.

. Fitri Wahyuni., *"The Basics of Indonesian Criminal Law"* Nusantara Persada Utama. Jakarta, 2017, p.35.

Firdaus Renuat et al*., Introduction to Criminal Law*, Editor: Dr. Parringotan Malau, S.T., S.H., M.H., (Padang: CV. Gita Lantera, 2023), p. 2.

Harun M. Husen., *"Crime and Law Enforcement in Indonesia"* Rineka Cipta. Jakarta. 1990. p.58.

Ismu Gunadi et al. *"Cepat Muda Understands Criminal Law"*.Jakarta: Achievements of Pustakaraya. 2011. p. 57.

Kristian Hutasoit. *"Juridical Review of Online Fraud in the Perspective of Criminal Law in Indonesia (Study of the Decision of the Banda Aceh District Court)".* Faculty of Law, University of North Sumatra, Medan, 2018. p. 4

Moch. Anwar, *Special Section of Criminal Law (Criminal Code Book II).* PT. Citra Aditya Bakti, Bandung. 1989, him. Sec. 62.

Moeljatno., *"Principles of Criminal Law"* Putra Harsa. Surabaya. 1993, p. 23

Moeljatno, *Principles of Criminal Law*, (Jakarta: Rineka Cipta, 2008), p. 45.

Niniek Suparni, 2009, *Cyberspace Problematics & Anticipation of Its Arrangements*, Sinar Grafika, Jakarta, p.31.

Ni Nyoman Triana Suskendariani and Sabri Guntur, *The Development of Mayantara Crime, Lakidende Law Review*, Vol. 1, No. 2, 2022, p. 121

P.A.F. Lamintang, *Basics of Indonesian Criminal Law*, (Bandung: Citra Aditya Bakti, 2013), p. 83

Sahariyanto, Budi, 2012*, Information Technology Crime (Cyber Crime) Urgency of Regulation and Legal Loopholes*, Rajawali Pers, Jakarta, him, 10.

Setia Untung Arimuladi, *Corporate Crime in Electronic Transactions*, Setara Press, Malang, 2021, p. 2.

Sitompul, Josua, 2012, Cyberspace, Cybercrimes, Cyberlaw: An Overview of Criminal Law Aspects, Rajawali Press, Jakarta, p.25.

Soerjono Soekanto, *Factors Influencing Law Enforcement*, Rajagrafindo, Persada, Jakarta, p. 5.

Soerjono Soekanto., *"Factors Affecting Law Enforcement*" UI Pres. Jakarta. 1983. p.35.
Wirjono Prodjodikoro, *Certain Criminal Acts in Indonesia*, Refika Adityama, Bandung, 2003, p. 36.
H. Dudung Mulyadi., *"Elements of Fraud in Article 378 of the Criminal Code Associated with Land Buying and Selling".* Vol.5, No.2. September. 2017. P.210.
I Gusti Made Jaya Kesuma et al, *Law Enforcement Against Fraud Through Electronic Media,* Journal of Legal Practice, Vol. 1, No. 2, 2020, p. 72
Nida Rafa Arofah and Yeni Priatnasari*, Internet Banking and Cyber Crime* : A Case Study in National Banking, Journal of Accounting Education, Vol. 18, No. 2, 2020, p 109
Randi Aritama., *"Fraud in Criminal Law and Civil Law".* Journal of Scientific Research. Vol.1, No.3 November. 2022. P. 728 ejournal.nusantaraglobal.ac.id/index.php/sentri.