

The Role of the Cyber Crime Unit of the North Sumatra Regional Police in Overcoming Online Fraud Crime in North Sumatra

Muhammad Hafizsyah¹⁾ & Zaid Alfauza Marpaung²⁾

¹⁾ Universitas Islam Negeri Sumatera Utara, Medan, Indonesia, E-mail: muhammadhafizsyah02@gmail.com

²⁾ Universitas Islam Negeri Sumatera Utara, Medan, Indonesia, E-mail: zaidalfauzamarpaung@uinsu.ac.id

Abstract. *The rise of online fraud crimes in North Sumatra has caused financial losses to victims. This study aims to determine the role of law enforcement of the cybercrime unit of the North Sumatra regional police and its obstacles to the perpetrators of online fraud. The method used is empirical legal research whose sources are obtained from primary, secondary and tertiary data which are then analyzed qualitatively. The results of the study found that significant challenges faced by investigators in handling online fraud cases. Difficulties in identifying perpetrators who use fake identities and often change places are the main obstacles that slow down case resolution. These obstacles show the complexity of the mode of operation used by the perpetrators, which requires sophisticated and adaptive handling strategies from the police. Preventive and repressive efforts carried out by the Cyber Unit of the North Sumatra Police Ditreskrimsus are the right steps in tackling online fraud. Strict supervision of social media, counseling to the public, and takedowns of content containing elements of fraud are proactive steps that can prevent further fraud. In addition, the resolution of outstanding reports demonstrates the police's commitment to providing a sense of security to the community. However, the success of this effort also depends on good cooperation between the community and the police. Continuous education to the public on the dangers of online fraud and how to prevent it is essential to reduce the number of victims. In this digital era, increasing the capacity and skills of investigators in information technology is also a crucial factor in dealing with increasingly sophisticated criminals. Overall, this study emphasizes the importance of a holistic and integrated approach in tackling online fraud crimes.*

Keywords: *Fraud; Online; Police; Role; Technology.*

1. Introduction

Advances in information technology have brought humans to the era of globalization, which makes various activities easy to do based on technology, such as communication, information and transactions. However, criminals can also take advantage of this advantage to commit criminal acts in various fields, especially in the internet media. This brings negative impacts such as defamation, pornography, online fraud, account breaches, data theft, virus attacks and online gambling.

Crime prevention aims to improve public safety and comfort. Information technology crimes are increasingly becoming prevalent in society, so various ways are needed to overcome them. The police carry out crime prevention efforts as preventive and repressive measures. However, these countermeasures require support from all parties in order to reduce the crime rate.

The police is an institution that carries out its functions and duties in connection with the attributes attached to individuals and agencies. The police as one of the law enforcement agencies other than judges and advocates play a very important role in enforcing criminal law, to apply a criminal offense in accordance with applicable law. Because basically before a criminal case is submitted to the prosecutor's office or even to the court, the police have the authority to investigate and investigate a criminal offense which has been given by the provisions of Law No. 8 of 1981 (the Criminal Code).¹

The police as an organ of government makes its duties inseparable from conditions that influence each other with various processes and formal policy pressures set by the authorities. Modern policing is among the challenges that cause the institution's activities to undergo major changes, especially with regard to the issue of police neutrality or independence in the flow of power.

Article 1 of Law No. 2 of 2002 on the Indonesian National Police states that policing is all matters relating to the functions and institutions of the police in accordance with statutory regulations. Furthermore, Article 5 states that: a. "The Indonesian National Police is an instrument of the State that plays a role in maintaining public security and order, enforcing the law, and providing protection, protection and services to the public in the context of maintaining domestic security" b. "The Indonesian National Police is the National Police which is a unit in carrying out the

¹ Agus Raharjo. (2022). Peran Kepolisian Dalam Menanggulangi Perjudian Online (Cyber Crime Gambling)(Studi Kepolisian Daerah Sumatera Utara). *Skripsi*, p. 1-50
<<https://repository.uhn.ac.id/handle/123456789/7987>>.

role referred to in paragraph (1)."

So based on the provisions of the article above, it can be concluded that the definition of the Indonesian National Police is a State Institution that carries out its functions and duties in maintaining the security and order of the State and acts as a law enforcer and provides protection, protection and community services.

To deal with information technology-based crimes, the Criminal Investigation Agency (BARESKRIM) of the National Police has a special unit, namely Directorate II Economic and Special Unit V IT and Cybercrime. This unit is tasked with overcoming various crimes involving information and communication technology. Apart from the central level, several regional police forces such as North Sumatra, East Java, Central Java, Bali, and Yogyakarta Special Region have also established special units in the field of information technology. These units aim to effectively tackle and deal with cybercrime in their respective regions. The North Sumatra Regional Police formed a special unit to overcome and solve information technology-based crimes or cyber units, namely subdit V / Cybercrime, which in subdit v has 4 units that handle cyber cases. Both online gambling crimes, hate speech crimes, pornography crimes, defamation crimes and online fraud. However, the focus of the research taken by the researcher this time is the crime of online fraud.

Online fraud is increasing along with the advancement of information and communication technology. In the context of Indonesian criminal law, online fraud falls under the regulation of Article 378 of the Criminal Code, which describes the use of deceit to influence others in transactions or payments. Modes of operation of online fraud such as phishing, scams, and online buying and selling fraud generally involve using the internet to deceive people with false information or unreal offers. Tackling online fraud requires collaboration between the government, internet service providers and the public to strengthen regulation, law enforcement and education. Educating the public about digital literacy and online transaction security is also crucial to reduce the risk of fraud. ²

One type of e-commerce crime is online fraud. The online fraud referred to in e-commerce is online fraud that uses the internet for business and trade purposes so that it no longer relies on a real conventional company base. Various modes of fraud through online media continue to emerge and the perpetrators are increasingly neat in smoothing out their actions in fraud, this can be seen from the many fake buying

² Jason Aaron Riado Simanungkalit, Raihan Hertadi, and Asmak ul Hosnah. (2024). Analisis Tindak Pidana Penipuan Online Dalam Konteks Hukum Pidana Cara Menanggulangi Dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, 4.2, p. 281–94 <<https://doi.org/10.37481/jmh.v4i2.754>>.

and selling websites that are made in such a way and offer various products at prices below normal prices, with the intention of attracting victims to buy, and there is also fraud by victimizing other people's accounts to be the place of the results of criminal acts of fraud with the modus operandi that the perpetrator has transferred to the seller's account more than the agreed price for various reasons and asked for the excess to be returned to his account, but in reality the money is the result of the perpetrator's fraud against the victim in another place where the perpetrator pretends.

Selling a certain item, and giving the victim's account number beforehand. Legal problems that are often faced in online fraud crimes are related to the delivery of information, communication, and or electronic transactions, namely in terms of evidence and matters related to legal acts carried out through electronic systems. Online fraud is in principle the same as conventional fraud. The difference is only in the means of action, namely using Electronic Systems (computers, internet, telecommunications devices). So legally, online fraud can be treated the same as conventional offenses regulated in the Criminal Code (KUHP). In addition to fraud via the internet, fraud via SMS (Short Message Service) is also regulated in Law No. 11 of 2008 concerning information and electronic transactions. The media used in SMS fraud is a cellphone which is one of the electronic media referred to in the ITE Law. This is in accordance with Article 1 number 2 of the ITE Law which reads as follows: "Information Technology is a legal action carried out using a computer, computer network, and / or other electronic media. The fraud article in the Criminal Code (hereinafter referred to as the Criminal Code) still cannot accommodate this, because usually the perpetrators of fraud through online media also use email facilities to connect with their victims, in this case whether email can be used as valid evidence and can be equated with paper letters like conventional fraud crimes in the real world. Law enforcement that has not been good related to criminal acts of fraud on online buying and selling transactions and regarding the difficulty of proof because electronic data is relatively easy to change, intercepted or falsified, the proof referred to here is general / conventional proof, namely provisions that contain guidelines on ways that are justified by law to prove the guilt charged to the defendant, There are evidentiary principles that state that things that are generally known do not need to be proven, one witness is not a witness and the defendant's confession is not enough to state that he is guilty. Then the next problem is the lack of readiness of the apparatus in the implementation of Law No. 11 of 2008 concerning Electronic Information and Transactions and the Criminal Code.

Proving online fraud offenses involving Information and Communication Technology automatically requires knowledge and expertise in the field of Information and

Communication Technology. Investigators are generally police officers who are trained in the field of law, not in the field of Information and Communication Technology. So that it has limitations in investigating online fraud crimes which can affect the handling of online fraud cases.³

From the total data on online fraud cases received by Subdit V of the Special Criminal Investigation Unit of the North Sumatra Police, which amounted to 593 reports from 2020-2024. It was found that online fraud cases have increased and decreased every year. This indicates that the increase in public awareness of data security is still quite low and shows that the number of cyber crimes is still increasing. Law enforcement institutions, namely the Special Criminal Investigation Directorate of the North Sumatra Regional Police, have an important role in law enforcement against cybercrime on social media, especially those handled by Subdit V / unit 4 cybercrime. Taking into account the information previously described, the main problem discussed by this research is how Subdit V Special Crimes or Cyber Crime Unit at the North Sumatra Regional Police plays a role in enforcing the law against online fraud crimes that occur in North Sumatra, both the efforts made and what obstacles are faced in the process of law enforcement against perpetrators of online fraud crimes in the North Sumatra Regional Police.

The purpose of this research is to find out how the role of law enforcement by the Cybercrime unit (Subdit V Reskrimsus) of the North Sumatra Police in enforcing the law against online fraud and to find out the obstacles faced in the process of law enforcement against perpetrators of online fraud in the North Sumatra regional police area.

2. Research Methods

This research applies empirical juridical method to collect relevant data. The data collected is primary and obtained through field research, especially through observation of the role of the Cyber Crime Unit of the North Sumatra Regional Police in tackling online fraud in North Sumatra. Primary data is supported by primary legal materials, such as official laws and regulations, as well as secondary legal materials that provide explanations and interpretations of primary and secondary legal materials. This method allows researchers to gain an in-depth understanding of how the role of the cyber crime unit works in dealing with online fraud in the North Sumatra region, while still referring to the existing legal framework. This method combines data collection through literature study and field study. Literature study is

³ Panca Ipunk Rahadjie, Ma'ruf Hafidz, and Andika Prawira Buana. (2022). Epektifitas Penyidikan Tindak Pidana Penipuan Secara Online. *Journal of Lex Generalis (JLS)*, 3.3, p. 404–17.

used to refer to relevant theories, principles, and thoughts related to the role of the Cyber Crime Unit of the North Sumatra Regional Police in tackling online fraud. Meanwhile, to obtain primary data, researchers conducted interviews with competent parties at the North Sumatra Regional Police Special Criminal Investigation Directorate or Cyber Crime Unit to discuss the research issues concerned.

3. Results and Discussion

3.1. Legal regulation of online fraud crimes in the North Sumatra region

Law functions as an instrument to change society or conduct social engineering. Through various regulations and policies implemented, the law plays a role in shaping individual and group behavior, directing social development, and addressing various community issues and conflicts. For example, laws on human rights are made to increase awareness and protection of the fundamental rights of every individual. In addition, strict environmental regulations aim to change consumption and production patterns to be more environmentally friendly.

Law can also be used to redress social and economic inequality, such as through anti-discrimination laws or social welfare programs. Thus, the law not only functions as a means of enforcing rules, but also as a driver of positive social change, creating a just, safe and harmonious society. However, to ensure that the law can function optimally in directing society towards goodness, not only legal provisions are needed, but also effective law enforcement. This indicates that legal regulations must be effectively implemented in legal practice. In other words, there must be a guarantee that law enforcement is carried out properly. Proper implementation of legal provisions is essential to ensure that the rules that have been drafted do not just become text on paper, but are also implemented in real life. Good law enforcement means legal certainty, where everyone is required to be equal before the law and their rights are protected in a fair and transparent manner. In addition, it includes the existence of effectively functioning institutions, oversight and accountability that ensure that law enforcement is not misused or abused. As such, good rule of law is the foundation of social justice and societal stability, creating an environment where the rule of law is respected and implemented consistently.

The implementation of the law is not only a task for statutory officials, but also part of the bureaucratic process that must be implemented properly. Especially in the case of online fraud, the realization and enforcement of the law plays an important role in preventing and cracking down on these crimes. In an effort to deal with

cybercrime cases, several articles in the Criminal Code (KUHP) can be applied using the extensive interpretation method, namely through parables and similarities, to criminalize cybercrime acts. The law can adapt to technological developments and new types of crimes that emerge in the digital world. Some articles in the Criminal Code that can be applied to address online fraud crimes include: Article 378 of the Criminal Code can be applied to cases of fraud by offering and selling counterfeit products or goods through advertisements on websites, then receiving money from buyers who are interested in the offer.

In Indonesia, criminal law serves as the main tool to deal with crimes. Criminal law is an integral element of Indonesia's legal order or politics, where it plays an important role in solving various problems and crimes that occur. The Criminal Code (KUHP) is the main component in the system of other laws and regulations relating to the crime of online fraud.

Regulation of online fraud is essential to protect people who transact electronically. Consumers who are victims of fraud can suffer financial losses and provide benefits to criminals. Online fraud falls under the category of illegal contents which is a misuse of information technology, which includes the dissemination of false information or data on the Internet. In addition, the information disseminated may also be considered unethical and may violate the law and disturb public order.⁴

Law No. 19 of 2016 on the amendment of Law No. 11 of 2008 on electronic information and transactions is in line with the Criminal Code. Several norms in the revised ITE Law adopt the Criminal Code while providing a detailed explanation of the previous ITE Law. This makes the ITE Law more accommodating in dealing with all issues related to technology-based criminal offenses by providing clear material and procedural provisions. Therefore, the ITE Law provides legal certainty in conducting information technology-based activities, especially in dealing with online fraud crimes.

Perpetrators of online fraud in Law No. 19 of 2016 concerning Electronic Transaction Information are sanctioned under Article 45 paragraph (2), which refers to the actions contained in Article 28 paragraph (1) regarding actions that harm consumers in electronic transactions, such as online-based fraud. These transactions involve the use of computers, computer networks, or other electronic media as described in Article 1 number 2 of the ITE Law. Article 28 paragraph (1) generally limits electronic transactions in law. Both Article 28 paragraph (1) of the ITE Law and Article 378 of

⁴ Amelia Amelia. (2023). Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online. *Jurnal Inovasi Global*, 1.1, p. 14–25 <<https://doi.org/10.58344/jig.v1i1.3>>

the Criminal Code regulate the crime of fraud, with the ITE Law stipulating more severe criminal sanctions, namely up to 6 years of imprisonment and/or a fine of up to IDR 1,000,000,000, compared to the Criminal Code which only applies a maximum prison sentence of 4 years and/or a maximum fine of Category V or IDR 500,000,000.⁵

3.2. The Cyber Crime Unit of the North Sumatra Regional Police (SU POLDA) has an important role in handling online fraud crimes

The police have a very important role in overcoming online fraud crimes. The police in tackling online fraud crimes. Has several preventive efforts (prevention) and repressive efforts (restoring). Preventive efforts are efforts that continue in overcoming, namely by not providing space for someone to commit online fraud crimes, for example, what the police do is guard, supervise, and patrol. patrol activities are called cyber patrols. Repressive efforts are repressive efforts (suppressing, curbing, restraining, or oppressing; and healing. If interpreted simply, repressive efforts aim to restore the disturbed balance.

According to Article 14 Paragraph (1) Letter g of the Police Act, the main task of the police is to investigate and prosecute all criminal offenses in accordance with the criminal procedure law and other laws and regulations. In addition, Article 15 Paragraph (1) of the Police Act states that Articles 13 and 14 regulate the authority of the police in handling the growth of community diseases and taking law enforcement actions against crimes and criminality in accordance with applicable regulations⁶.

The police formed a special unit that deals with technology-based crime issues in each regional police force. The North Sumatra Regional Police formed a special unit to overcome and solve information technology-based crimes or cyber units, namely subdit V / Cybercrime, which in subdit v has 4 units that handle cyber cases. From the number of reports on criminal cases of information technology-based crimes, online fraud is number 2 with the most reports after insults and defamation from the data on reports received by Subdit V Cyber in the Special Criminal Investigation Unit of North Sumatra Police in 2020-2024. Then several efforts were made, namely

⁵ Aina Aurora Mustikajati and others. (2024). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Berdasarkan Perspektif KUHP Dan Undang-Undang Informasi Dan Transaksi Elektronik Terhadap Harta Benda Orang Yang Diatur Dalam Pasal 378 Buku II Bab XXV KUHP Kemudian Pemerintah Menetapkan Unda'.

⁶ Josia. (2020). Penegakan Hukum Yang Dilakukan Oleh Polri Terhadap Tindak Pidana Pencemaran Nama Baik Di Media Sosial. *Skripsi*, p. 5.

1. Preventive measures

Preventive efforts of the North Sumatra Regional Police include initial steps to prevent, mitigate, or reduce the incidence of crime. These include:

- a) appeal to the community through banners.
- b) provide legal counseling to the community, and
- c) conducting counseling through social media such as Instagram and other media.

To improve prevention efforts, the Police as a whole handles online arisan fraud cases based on the Criminal Code and ITE Law. Recently, the National Police Chief issued Circular Letter SE/2/11/2021 to promote awareness of ethical culture in Indonesia's digital space, especially regarding ITE crimes such as hate speech with the principle of restorative justice, but not for online fraud crimes regulated in Article 28 paragraph (1) and Article 45A paragraph (1).

Preventive efforts made by the North Sumatra Regional Police to tackle online fraud include socialization to the public to be more careful in electronic transactions, monitoring suspicious accounts on social media, and closing or blocking accounts that are involved or have the potential to commit fraud. Cooperation with the community is also emphasized to keep an eye on potential perpetrators of online arisan fraud. This preventive effort is important to limit opportunities for security and public order disturbances. In maximizing this effort, cooperation between parties such as the government, police, and social media providers is needed. Although the regulations in Indonesia are already comprehensive, there is a need to further strengthen the legal principles related to online-based fraud in the ITE Law.

2. Repressive measures

Repressive efforts are steps to restore order that is disturbed due to violations or crimes, by imposing sanctions in accordance with the type of offense or crime that occurred. This action is carried out by strictly enforcing the law in accordance with the applicable regulations against the perpetrators of the crime, so that it can be an example for the community to think more than once before committing a crime.⁷

⁷ Obby Michael Angelo, Erdianto Erdianto, and Erdiansyah Erdiansyah.(2015). Penegakan Hukum Penipuan Dengan Modus Online Shop Melalui Blackberry Messenger Berdasarkan Undang-Undang

This effort is carried out after the occurrence of a criminal offense or crime with the aim of enforcing the law through the application of punishment. The repressive approach is a crime prevention strategy that is carried out after a crime has occurred. Repressive measures aim to take action against the perpetrators in accordance with their actions and to change their behavior to realize that their actions violate the law and harm society. This is so that they do not repeat their actions and also as a warning to others about the severe consequences they will face if they do something similar.⁸

The action was carried out by investigators of Subdit V Ditreskrimsus Polda Sumut against online fraud cases, after prevention efforts were made but there were still violations of the law. This legal process is in accordance with the provisions of the applicable laws, such as Article 28 paragraph (1) jo Article 45A paragraph (1) of Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, as well as Article 378 of the Criminal Code which regulates criminal acts of fraud. Law enforcement steps begin with investigation, investigation, examination, and submission of cases to the Public Prosecutor (JPU), as revealed in the results of an interview with Kanit 4 of the Cyber Unit of the Special Criminal Investigation Unit of the North Sumatra Police.⁹

Law enforcement against perpetrators of fraud in online arisan through a repressive approach involves several stages, starting from the investigation. This action is carried out after a source of action such as a report, complaint, officer's own knowledge, or direct arrest. After the source of action is identified, the next step taken by the police is to conduct an investigation. In general, investigation or what is often referred to as research is the first step to determine the truth of a criminal event. According to Article 1 point 5 of Law No. 8 of 1981 concerning Criminal Procedure Law, "Investigation" refers to a series of investigator actions to search for and identify an event suspected of being a criminal offense, with the aim of determining whether an investigation is necessary in accordance with the provisions of the applicable law. Article 1 point 5 explains that investigation includes efforts to seek evidence and information to assess whether an action or event can be

Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Oleh Penyidik Ditreskrimsus Kepolisian Daerah Sumatera Utara. *JOM Fakultas Hukum*, 4.2, p. 1–15.

⁸ Rizka Sofianti. (2021). *Upaya Kepolisian Dalam Mencegah Penipuan Arisan Online*. Bandung Conference Series: Law Studies, 1.1, p. 12–16.

⁹ Dyna Glory Mangerongkonda and Merry Elisabeth Kalalo. (2022). *Tanggung Jawab Pidana Dan Perdata Terhadap Pelaksanaan Arisan Online*, 8.1.

classified as a violation of the law based on existing laws or regulations.¹⁰

From the number of online fraud cases totaling 593 reports from 2020-2024 with the number of completed reports totaling 223 with details:

Table 1. Data on Crime in Subdit V Cyber Ditreskrimsus Polda North Sumatra Year 2022-2024

Year	Number of Reports	Number of Completed Reports
2020	170	11
2021	93	51
2022	105	62
2023	121	86
2024	104	13
Total	593	223

Based on the table above, online fraud in the jurisdiction of the North Sumatra Regional Police in 2020 was 170 case reports and 11 cases were successfully resolved, then in 2021 it decreased, namely 93 case reports and 51 completed reports, in 2022 it increased, namely 105 and 62 completed reports, then in 2023 it increased, namely 121 with 86 completed reports, and in 2024 there was a slight decrease from the number of cases in 2023 with 13 completed cases.

This is a significant concern for the cyber unit in completing reports that are still largely unresolved with reports of the number of online fraud cases with the modes and methods used by the perpetrators increasingly developing by following the era of modern times. Which requires assistance and cooperation from both the community and other agencies. Investigators at the North Sumatra Regional Police explained that another activity carried out by the regional police to deal with cybercrime is monitoring sites that contain pornographic content and online gambling. They work closely with the Ministry of Communication and Information to block sites that violate the law, as part of efforts to prevent the spread of public diseases and ensure safe internet access for the community. These efforts are supported by optimizing resources to deter and stop criminal acts, especially those related to cybercrime.¹¹

3.3. Obstacles and constraints faced by the cyber crime unit of the North Sumatra regional police in tackling online fraud criminal acts

There are several obstacles faced by the North Sumatra Regional Police in tackling

¹⁰ Tamimi Pratiwi. (2018). Pelindungan Hukum Terhadap Tindak Pidana Penipuan Arisan Online. p. 1–74.

¹¹ Ruth Gladys Sembiring and others. (2023). Penegakan Hukum Cybercrime Di Wilayah Hukum Kepolisian Daerah Sumatera Utara. *Locus Journal of Academic Literature Review*, 2.3, p. 292–304.

criminal acts of fraud including:

1. Investigators at the North Sumatra Police face internal constraints such as limited human resources and facilities when conducting investigations. Before starting an investigation, they conduct an investigation as the first step to gather sufficient preliminary evidence. The function of investigation is not only to determine whether an act constitutes a criminal offense, but also as a protection of human rights and to ensure the use of coercive tools in accordance with legal provisions. However, in dealing with crimes such as online fraud that increasingly use technology, obstacles arise from the limited number of investigative teams and inadequate facilities. Handling cases involving electronic transactions is also increasing, requiring more human resources and more sophisticated facilities to track down perpetrators who may be in a different location to the victim. Therefore, it is important for the government to improve the facilities and tools available to the police to be more effective in dealing with crimes through social media, such as online fraud. This will help in the prevention of crimes before they occur and allow cybercrime investigators to better handle more complex cases.

2. External constraints in law enforcement against online fraud perpetrators are strongly influenced by public attitudes. Although many cases of online arisan fraud have been revealed, there are still many victims who are reluctant to report to the police because they are embarrassed or do not have strong enough evidence. As a complaint offense, law enforcement against fraud requires reporting from victims to be able to carry out arrests, legal proceedings, and prosecutions that can provide a deterrent effect on the perpetrators of crime. The important role of criminology in complementing criminal law related to law enforcement efforts is not only limited to the prosecution aspect, but also in understanding the reasons behind criminal acts. The public needs to be more aware of the lure of big profits online, and be wiser in making transactions on social media, especially if the executor's account is unknown. The North Sumatra Regional Police hopes that the public will participate in monitoring and reporting potential online fraud to reduce the number of victims. The perpetrators are reminded not to repeat their actions that harm others, while the public is expected to be more aware of various forms of fraud that may occur. People should be active in keeping an eye out for potentially suspicious neighbors on social media, as online scams often target people they know to make them easier to trick. This external obstacle from the community greatly impacts the results of police investigations, because without community cooperation, it is difficult for

the police to track down online fraudsters who can be anywhere using social media accounts.¹²

The results of an interview with the head of unit 4 of subdit V cyber at the special police headquarters, AKP Vicktor R.P Pasaribu, S.H., M.H. He said that the number of reports received by investigators sometimes takes a little longer to complete so that reports in 2020 are completed in the following year due to the difficulty of finding perpetrators who use fake identities and change places in committing their crimes and the obstacles faced depend on the methods and modes used such as the example of online arisan cases that use the same account number so that it helps a little in finding the perpetrators but for online fraud cases with the mode of selling cars in the marketplace that use different identities and accounts where the perpetrators use people's identities to create accounts with various lures to people who want to use their identities. Mr. AKP Vicktor R.P Pasaribu, S.H., M.H. along with the cyber unit of the North Sumatra Police Special Crimes Unit continue to monitor social media related to posts that contain elements of fraud, conduct counseling to the public and provide counseling to campuses and improvements in handling online fraud crimes both takedown and continue to complete unresolved reports to provide a sense of security to the community, He hopes that the community will be more careful in providing identity to other people on behalf of providing any form of assistance and can help reduce this criminal fraud by reporting the incident to the police station then better understand and know the characteristics of online fraud crimes and other crimes so that they can help the police in tackling these crimes starting from themselves, family and others.

4. Conclusion

The police play a very important role in criminal law enforcement, to apply a criminal offense in accordance with applicable law. Therefore, the ITE Law provides legal certainty in conducting information technology-based activities, especially in dealing with online fraud crimes. In tackling the crime of online fraud, the North Sumatra Regional Police also made preventive efforts as an initial step to prevent, overcome, or reduce the incidence of criminal acts. By providing appeals to the public through banners, providing legal counseling to the public, and conducting counseling through social media such as on Instagram and other media.

¹² Khairul Fahmi Gultom. (2022). Analisis Kriminologi Terhadap Pelaku Tindak Pidana Penipuan Dengan Modus Arisan Online (Studi Pada Kepolisian Resor Kota Besar Medan). *JIMHUM: Jurnal Ilmiah Mahasiswa Hukum*, 2.1, p. 1-17.

5. References

- Amelia. (2023). Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online', *Jurnal Inovasi Global*, 1.1, p. 14–25 <<https://doi.org/10.58344/jig.v1i1.3>>
- Angelo, Obby Michael, Erdianto Erdianto, and Erdiansyah Erdiansyah. (2015). Penegakan Hukum Penipuan Dengan Modus Online Shop Melalui Blackberry Messenger Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Oleh Penyidik Ditreskrimsus Kepolisian Daerah Sumatera Utara. *JOM Fakultas Hukum*, 4.2, p. 1–15
- Gultom, Khairul Fahmi. (2022). Analisis Kriminologi Terhadap Pelaku Tindak Pidana Penipuan Dengan Modus Arisan Online (Studi Pada Kepolisian Resor Kota Besar Medan). *JIMHUM: Jurnal Ilmiah Mahasiswa Hukum*, 2.1, p. 1–17
- Josia. (2020). Penegakan Hukum Yang Dilakukan Oleh Polri Terhadap Tindak Pidana Pencemaran Nama Baik Di Media Sosial. *Skripsi*, p. 5
- Mangerongkonda, Dyna Glory, and Merry Elisabeth Kalalo. (2022). Tanggung Jawab Pidana Dan Perdata Terhadap Pelaksanaan Arisan Online', 8.1.
- Mustikajati, Aina Aurora, Alamat Jalan, Ir Sutami, and Jawa Tengah. (2024). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Berdasarkan Perspektif KUHP Dan Undang-Undang Informasi Dan Transaksi Elektronik Terhadap Harta Benda Orang Yang Diatur Dalam Pasal 378 Buku II Bab XXV KUHP Kemudian Pemerintah Menetapkan Unda. 1.2 .
- Pratiwi, Tamimi. (2018). Pelindungan Hukum Terhadap Tindak Pidana Penipuan Arisan Online, p. 1–74
- Rahadjie, Panca Ipunk, Ma'ruf Hafidz, and Andika Prawira Buana. (2022). Epektifitas Penyidikan Tindak Pidana Penipuan Secara Online. *Journal of Lex Generalis (JLS)*, 3.3, p. 404–17
- Raharjo, Agus.(2022). Peran Kepolisian Dalam Menanggulangi Perjudian Online (Cyber Crime Gambling)(Studi Kepolisian Daerah Sumatera Utara. *Skripsi*, p. 1–50 <<https://repository.uhn.ac.id/handle/123456789/7987>>
- Rizka Sofianti. (2021). Upaya Kepolisian Dalam Mencegah Penipuan Arisan Online', *Bandung Conference Series: Law Studies*, 1.1, p. 12–16



Jurnal Daulat Hukum
Volume 7 No. 2, June 2024
ISSN: 2614-560X
SINTA 3 Decree No.
0547/ES/DT.05.00/2024
Dated May 15, 2024

The Role of the Cyber Crime Unit....
(Muhammad Hafizsyah & Zaid Alfauza Marpaung)

<<https://doi.org/10.29313/bcsls.v1i1.80>>

Sembiring, Ruth Gladys, Madiasa Ablisar, Mahmud Mulyadi, and Jelly Leviza. (2023). Penegakan Hukum Cybercrime Di Wilayah Hukum Kepolisian Daerah Sumatera Utara. *Locus Journal of Academic Literature Review*, 2.3, p. 292–304

Simanungkalit, Jason Aaron Riado, Raihan Hertadi, and Asmak ul Hosnah. (2024). Analisis Tindak Pidana Penipuan Online Dalam Konteks Hukum Pidana Cara Menanggulangi Dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, 4.2, p. 281–94 <<https://doi.org/10.37481/jmh.v4i2.754>>.