Formosa Journal of Social Sciences (FJSS)
Vol.3, No.2, 2024: 287-300

# Digital Evidence Tracing in the Investigation of Identity Theft in the E-Commerce Era

Shinta Widhaningroem[1*], Yeni Widowaty[2]
Universitas Muhammadiyah Yogyakarta
**Corresponding Author:** Shinta Widhaningroem shintawdhh@gmail.com

A R T I C L E I N F O

*Keywords:* Investigations, Criminal Acts, Identity Theft, E-Commerce, Cybercrime

*Received : 11 April*
*Revised : 17 May*
*Accepted: 21 June*



A B S T R A C T

This research analyzes the application of regulations in prosecuting cyber crime in identity theft on e-commerce platforms in Indonesia. This study uses normative juridical research methods. This research considers various relevant laws, such as the Information and Electronic Transactions Law (UU ITE), the Criminal Code (KUHP), the Copyright Law, the Telecommunications Law, the Company Documents Law, and the Money Laundering Crime Law. Analysis shows that this law provides a strong legal basis for law enforcement to take action against cybercriminals and impose appropriate criminal sanctions. Apart from that, the law regulates electronic evidence, strengthening the investigation process against perpetrators. However, prosecuting cybercrime cases of identity theft on e-commerce platforms often experiences obstacles, especially in arresting suspects and confiscating evidence. This is due to the characteristics of digital crimes which are often complex and difficult to trace, as well as the lack of adequate capabilities and resources on the part of law enforcement in handling these types of cases. Greater efforts are needed to increase law enforcement capacity, as well as closer cooperation between authorities and e-commerce platform providers to increase the effectiveness of law enforcement in dealing with cybercrime

DOI: https://doi.org/10.55927/fjss.v3i2.9797
ISSN-E: 2830-0246
https://journal.formosapublisher.org/index.php/fjss

## INTRODUCTION

The digital era brings significant changes in the way people shop. E-commerce platforms such as Shopee, Lazada, and Tokopedia, offer ease and convenience in buying various needs. However, behind these conveniences, there is a potential for criminal acts that need to be watched out for.

Criminal acts in online transactions can occur in various forms, such as fraud (Article 378 of the Criminal Code), theft (Article 362 of the Criminal Code), embezzlement (Article 372 of the Criminal Code), counterfeiting (Article 263 of the Criminal Code), destruction of goods, transaction errors, inconsistencies in goods, and payments that are not made.

Fraud in online transactions is rampant, where sellers deceive buyers by offering counterfeit goods, not delivering goods after receiving payment, or using buyers' personal data to carry out other criminal acts. This is emphasized in Article 28 paragraph (1) of the ITE Law regarding fraud through electronic media (Kamran & Maskun, 2021). Personal data theft is also a troubling modus operandi. Sellers can steal a buyer's credit or debit card information and use it to enter into transactions without approval. The criminal act is regulated in Article 32 paragraph (1) of the ITE Law concerning criminal acts against computer systems (Malalangi, 2022). In addition, embezzlement is also frequent, where the seller receives payment from the buyer but does not deliver the goods or return the buyer's money. This is regulated in Article 372 of the Criminal Code concerning embezzlement (Hartanti, Titahelu, & Taufik, 2021). Product counterfeiting is also rampant, where sellers sell counterfeit goods or imitate well-known brands. This is regulated in Article 263 of the Criminal Code regarding forgery (Wittadarma, Sugiartha, & Widyantara, 2022). Destruction of goods can also occur, where the goods that have been received by the buyer are damaged or not in accordance with the advertised conditions. Transaction errors are also common, such as the buyer entering the wrong shipping address or the number of items purchased. The non-conformity of the goods is also a problem that is often faced by buyers, where the goods that have been received do not match the description that has been given by the seller. The absence of payment is also a frequent problem, where buyers order goods but do not make payments. Identity theft in e-commerce is indeed part of cyber crime. These crimes involve the unauthorized use of a person's personal information for fraudulent purposes or other illegal activities. Actors can obtain personal information, such as names, addresses, credit card numbers, and other identification numbers, through various methods such as phishing, malware, or database hacking (Cassim, 2015).

This identity theft has a significant impact, not only making the victim financially harmful, but also damaging the reputation and security of the e-commerce platform itself. Perpetrators can use the stolen information to make unauthorized purchases, open new bank accounts, or engage in other fraudulent activities. As a result, victims often face large financial losses and a lengthy recovery process to restore their identities and clear their financial records.

## LITERATURE REVIEW

According to Maulana (2024), "criminal acts in online transactions are increasingly rampant and cause losses for many parties. Thus, it is necessary to take strict prevention and enforcement efforts to protect the rights of consumers and business actors in this digital era". Budiman, Rifai, & Senda (2023) stated that it is necessary to carry out education and socialization to the public regarding the law related to online transactions. This is important to increase public awareness of potential criminal acts in online transactions and encourage them to make online transactions safely and responsibly.

Humanity has entered the digital age as a result of the advancement of science, knowledge, technology, and art. This led to the creation of the internet, a global network that connects network subsystems to form a huge network that can be connected online. The convergence of data, information, music, and images through internet technology has the potential to affect human life (Widodo, 2013).

Nowadays it is common to need and use the Internet for everything from e-banking and e-commerce to e-Government and e-education, as well as many other professions. Even though people, especially those living in big cities, may not know about information technology problems, they are still considered GAPTEK or outdated. Cyberspace is a new world created by the internet. It is a computer-based field of communication that provides virtual reality (indirect and unreal) (Saputra, 2023). With just a few pushstrokes of a button, anyone can connect, communicate, and transact business with people thousands of kilometers away, even if it's all done virtually. This is achieved by radically changing the perception of time and distance provided by the Internet.

Large computer networks and the internet are not too disruptive to humans; Instead, they can be used for purposes that are more beneficial to society. Take the banking industry, for example, where e-banking allows us to make banking transactions whenever we want and e-commerce facilitates the purchase or sale of goods easily without requiring us to know where the goods are. With the existence of e-libraries and various other conveniences made possible by the growth of the internet, it is not difficult to find references or information about science. However, internet users feel uneasy because there is a human element that exploits the internet for bad purposes. Humans are referred to as black hackers or crackers, while this crime is known as cybercrime. The word "hacker" literally means "to cut or slice". Another way to characterize hackers is those who enjoy learning and experimenting with computer systems.

The definition of "hacker" is refracted here, but the use of the term has evolved as the internet has grown. First, there are white hat hackers who adhere to the same belief as their predecessors, namely that hacking should only be done to strengthen network security. online. Meanwhile, those who use their skills to commit crimes—such as stealing credit card details or damaging other people's websites—are referred to as crackers, or "black hackers." (Putri, 2020).

The forms of cybercrime can be categorized into seven, including: "Unauthorized Access to Computer; Illegal Contents; System and Service; Cyber Espionage; Data Forgery; Cyber Sabotage and Extortion; Infringements of

Privacy, Offense against Intellectual Property" (Habibi & Liviani, 2020; Sari, 2014; Sartika, Siregar, & Kartika Sari, 2020). The application of regulations on the ensnaring of cybercrime in identity theft on e-commerce platforms in Indonesia involves several relevant laws, especially the Electronic Information and Transaction Law (UU ITE). Articles in the ITE Law, such as Article 30 concerning illegal access to computer or electronic systems, and Article 46 concerning data theft, are the legal basis for handling cases of digital identity theft.

Digital evidence tracing in the investigation of identity theft crimes in the e-commerce era plays a key role in gathering strong evidence to prosecute criminals. The process begins with the identification and collection of relevant digital data from various sources, including e-commerce platforms, servers, and electronic devices involved in the crime. This digital evidence can be transaction records, activity logs, conversations, and other digital traces that can help identify the perpetrator and strengthen the case (Fadli, Widijowati, & Andayani, 2024).

## METHODOLOGY

Normative legal research or normative juridical research methods are used in this study. Legal research that sees law as an arrangement of interrelated norms, such as principles, norms, rules of laws and regulations, court decisions, agreements, and doctrines (doctrines), is referred to as normative legal research (Dewata & Achmad, 2017)

Secondary data will be an important component of this study. The researcher collected data from various sources such as police reports, legal journals, and scientific literature related to identity theft crimes on e-commerce platforms in Indonesia. These data will be analyzed in depth to provide a comprehensive picture of the current conditions related to identity theft on e-commerce platforms, including trends, patterns, and characteristics of existing cases. This data analysis will be the basis for compiling findings and conclusions in journal articles.

This research method will be carried out systematically and structured. First, the researcher will conduct a literature review to gather relevant information about the applicable legal framework and previous research related to identity theft crimes on e-commerce platforms. Furthermore, the researcher carried out an analysis on relevant laws and regulations, including the ITE Law, the Criminal Code, and regulations related to consumer protection.

## RESULTS AND DISCUSSION

Investigation Process of Cyber Crime Identity Theft in e-Commerce in Indonesia

Identity theft in e-commerce is part of cyber crime. This involves using a person's personal data without permission for fraudulent purposes or other illegal activities. In the realm of e-commerce, perpetrators can obtain sensitive information such as credit card numbers, email addresses, and passwords through various methods such as phishing, malware, or website hacking (Fadli, Widijowati, & Andayani, 2024).

The investigation process into identity theft in e-commerce involves specific steps to identify the source of the data leak and trace the digital footprint of the perpetrator. Investigators typically work closely with e-commerce service providers and banks to examine suspicious transactions and identify unusual usage patterns. Digital evidence such as access logs, transaction records, and metadata from devices used are often important tools in these investigations.
The procedure for investigating identity theft or cybercrime on e-commerce platforms is essentially the same as processing other traditional crimes, with a few exceptions. For example, the equipment used to commit crimes is a special unit called a cyber unit. In addition, managing cybercrime investigations is more difficult because it requires close coordination with other related organizations (Agus & Riskawati, 2016). In conducting an investigation, investigators go through a series of stages which include investigation, prosecution, examination and completion of case files.

1. Investigation

The investigation stage is the first and most challenging stage in the investigation process because it determines the type of police report to be submitted by requiring investigators to provide evidence about the crime, its methods and causes.

The process of investigating cybercrime identity theft on e-commerce platforms in Indonesia begins with a report by the victim or a party who feels aggrieved. Once the report is received, the cybercrime unit of the police will conduct an initial assessment to ensure the validity of the report and determine the necessary investigative steps. At this stage, the initial identification of the modus operandi of identity theft is carried out to understand how the victim's data can be stolen, whether through phishing, malware, or system hacking.
Usually, a notification letter or report from a foreign country is received by the NCB/Interpol, which then forwards it to the assigned cybercrime unit. The procedures used in researching cybercrimes involving carding cases are almost the same as those used in investigating drug-related crimes, especially in the fields of disguise and delivery of control.

Officers work closely with delivery partners to deliver products after receiving information or reports from Interpol or retailers who have suffered losses. The problem in a situation like this is that the report is received after the bank refuses to pay for the goods, meaning that the goods have been received by the perpetrator. In addition, the carder officer and the shipping employee work together, so if the police cooperate, information will be leaked and the perpetrator cannot be arrested because of his identity. Most of the ones listed are fake. Investigating suspected hacking or illegal access to someone else's computer network and making changes (defacement) is fraught with difficulties, especially when it comes to evidence. It is very difficult to conduct investigations and take action because many witnesses and suspects are not under Indonesian law. This is in addition to the challenging evidence problems related to information technology and digital codes, which require forensic computer equipment and human resources.

2. Enforcement

The prosecution of cybercrime cases of identity theft on e-commerce platforms involves a series of steps starting from early surveillance and detection by authorities and e-commerce platforms. E-commerce platforms typically have security systems in place to detect suspicious activity, such as unusual login attempts, unusual transaction patterns, or inconsistent data usage. When suspicious activity is detected, the platform can take quick action such as freezing the indicated account or informing the user for identity verification.

Once a report is received from the victim or detected by the platform's security system, the authorities, particularly the cybercrime unit of the police, will initiate an investigation. It involves collecting digital evidence, analyzing data, and tracking the perpetrator's online activities. The authorities will work closely with e-commerce platforms and internet service providers to obtain the necessary data. During this process, extra security measures are also implemented to protect the victim's data and prevent further losses. Digital forensic experts play a crucial role in analyzing evidence and ensuring the integrity of the data collected.

If sufficient evidence has been collected, the action will continue with the identification of the perpetrator and the arrest. The police will identify the suspect based on the available evidence and make an arrest if necessary. After the perpetrator is arrested, the legal process continues with the preparation of the case file which is submitted to the prosecutor's office for prosecution. Throughout this process, the authorities work to ensure that all legal procedures are followed correctly, and that the perpetrator is sentenced accordingly in court. This action aims not only to provide justice for victims, but also to provide a deterrent effect and prevent similar crimes in the future.

However, there are often challenges in prosecuting identity theft cybercrimes on e-commerce platforms, especially when arresting suspects and confiscating evidence. Because they only use computers to make arrests, which can be made anywhere without anyone's knowledge, and because there are no witnesses who can see the crime firsthand, authorities are often unable to identify the real perpetrators when apprehending the criminals. Only the IP address of the perpetrator and the computer he or she is using can be found in the farthest tracking results.

If the perpetrator uses an internet café, this will be even more difficult because, nowadays, these places almost never register their customers, making it impossible for us to determine who is using the computer when a crime occurs. The seizure of evidence is fraught with difficulties because, in many cases, the whistleblower is slow to report. This implies that the attack data in the server logs has been deleted, which is common in deface cases. As a result, investigators find it difficult to find statistical logs on the server because the server usually deletes them automatically. logs already exist to reduce server load. In contrast to statistical log data which is important evidence in hacking cases to ascertain the direction of the attack, this shows that investigators cannot find the necessary data to be used as evidence.

3. Examination

Examining identity theft cybercrime cases on e-commerce platforms requires a comprehensive and thorough approach. This examination process involves the collection of strong digital evidence, in-depth analysis of crime patterns, and the identification of perpetrators through the digital footprint left behind. Authorities such as the cybercrime unit of the police are working closely with e-commerce platforms and internet service providers to access relevant data. This data includes activity logs, transaction records, as well as information from devices used by victims and perpetrators.

It is difficult to apply legal provisions in cybercrime cases. One of the major problems that is quite concerning is the application of articles imposed on cybercrime cases on identity theft crimes on e-commerce platforms. For example, can a hacker who steals data be held accountable under Article 362 of the Criminal Code? This article demands that all or most of the property belonging to others be lost, even if the data stolen by hackers does not change at all. Because there are individuals who use the data for personal interests or know company secrets, usually this is only revealed after a long time. There are several obstacles in the examination of victims and criminal acts because there are no witnesses present at the time the criminal act is committed (testimonium de auditu). They only learn about the attack after it has occurred, as hacking attacks often result in a change in appearance or the malfunction of an already installed program.

Theft is defined as the seizure of other people's property with the aim of owning it illegally. Article 362 of the Criminal Code regulates theft. Article 362 of the Criminal Code may not apply in the context of cybercrime because digital data is often not considered a "good" in the traditional sense. Therefore, it is more appropriate to use articles from the ITE Law (Electronic Information and Transaction Law). For example, illegal access to computers or electronic systems is regulated in Article 30 of the ITE Law, which is more suitable in situations involving identity or data theft.

To ensure proper law enforcement, law enforcement must use a legal framework that is specific to cybercrime. Article 46 of the ITE Law establishes sanctions for those who illegally access and take data, with severe criminal threats. Thus, although Article 362 of the Criminal Code can be difficult to apply directly to cases of digital identity theft, the combination of articles in the ITE Law provides a strong legal basis for cracking down on cybercrime perpetrators. Effective examination and enforcement require a deep understanding of cyber law and information technology to ensure justice for victims and the prevention of future crimes.

4. Settlement of case files

The problem of evidence arises when the investigation has been completed and documented in the case file because law enforcement officials do not always view digital evidence in the same way. Digital evidence includes identity theft crimes committed on e-commerce platforms and cybercrimes for which there is currently no exact definition. differs in its conclusion due to the fact that digital evidence is not necessarily in actual physical form. For example, in the case of murder, the main evidence is usually the knife used in the crime;

However, in the case of cybercrime, such as identity theft on e-commerce platforms, the main evidence is usually a computer, but the computer itself is only physical, and the data on the computer's hard drive is the most important. which is in the form of a file and if printed will require a lot of paper to print it. Alternatively, the evidence can be contained on a compact disc. Until now, there is no legal framework that regulates the format of digital evidence that can be used as evidence in trials.

The settlement of identity theft case files on e-commerce platforms is an important stage in the legal process that ensures justice for victims and takes action against cyber criminals. After the investigation is complete and sufficient evidence has been collected, the case file is compiled by the authorities, usually by the cybercrime unit in the police. This case file contains all relevant information including digital evidence, investigation reports, and identification of suspects and victims.

Furthermore, the case file was submitted to the prosecutor's office for prosecution in court. At this stage, the prosecutor will review the case file and decide whether or not the case is worthy of being examined in court. If feasible, the prosecutor will prepare an indictment containing charges against the suspect based on the evidence gathered during the investigation.

In court, the trial process will be carried out to decide whether the suspect is guilty or not and determine the appropriate punishment. During the trial, the prosecutor will present various available evidence to provide evidence of the criminal act committed by the suspect, while the defense lawyer will defend the suspect. The judge will consider all the evidence and arguments presented before making a final decision.

Application of rules in the Ensnaring of Cyber Crime in Identity Theft on E-Commerce Platforms in Indonesia

The application of regulations in ensnaring cyber crimes in identity theft on e-commerce platforms in Indonesia involves several relevant laws, especially the Electronic Information and Transaction Law (UU ITE). Articles in the ITE Law, such as Article 30 concerning illegal access to computer or electronic systems, and Article 46 concerning data theft, are the legal basis for handling cases of digital identity theft.

Criminal legal measures, such as the application of criminal penalties against those who commit crimes that fall within the scope of cybercrime and identity theft on e-commerce platforms, can be used to combat crime in society, including cybercrime (Anthony, 2018). Sanctions for cybercrime perpetrators include the following: Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Information and Electronic Transactions which specifically regulates the criminal formulation of cybercrime; Several other laws and regulations also contain content related to cybercrime.

**Law No. 11 of 2008 Jo Law No. 19 of 2016 Concerning Information and Electronic Transactions**

As stipulated in the Criminal provisions in Chapter XI of the ITE Law, it is stated that acts that are criminally threatened with cybercrime, identity theft crimes on e-commerce platforms related to information and electronic transactions include the following:

a. Article 45 paragraph (1) of the ITE Law; Any person who without the right to distribute and/or make accessible electronic information and electronic documents containing moral content shall be sentenced to imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000 (one billion rupiah). Article 45 paragraph (2) ; any person who without rights spreads false and misleading news; disseminate information aimed at inciting hatred; sentenced to imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000 (one billion rupiah). Article 45 paragraph (3) ; Any person who without the right to send / electronic documents and/or electronic information containing threats of violence aimed at personally is sentenced to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of Rp. 2,000,000,000 (two billion rupiah).
b. Article 46 of the ITE Law; any person who without the right to access another person's computer network shall be sentenced to imprisonment for a maximum of 6 years and/or a fine of Rp. 600,000,000 (paragraph 1); imprisonment for a maximum of 6 years and/or a maximum fine of Rp. 1,000,000,000 (paragraph 2) and a maximum penalty of 12 years and/or a maximum fine of Rp. 2,000,000,000,-
c. Article 47 of the ITE Law; every person who does not have the right to intercept is sentenced to imprisonment for a maximum of 10 years and/or a maximum fine of Rp800,000,000,-
d. Article 48 of the ITE Law; Any person who unlawfully alters, adds, reduces, transmits, damages, deletes, moves, conceals other people's electronic information and/or electronic documents or public property in any way shall be sentenced to imprisonment for a maximum of 8 years and/or a maximum fine of Rp.2,000,000,000,- (paragraph 1). Any person who unlawfully transfers or transfers electronic information and/or electronic documents to the electronic system of another person who is not entitled to be sentenced to imprisonment for a maximum of 9 years and/or a maximum fine of Rp. 3,000,000,000 (paragraph 2). Any person who carries out the actions as described above and results in the disclosure of confidential or personal information shall be punished with imprisonment for a maximum of 10 years and/or a maximum fine of Rp. 5,000,000,000,.
e. Article 49 of the ITE Law; every person who unlawfully commits an act that results in the disruption of the electronic system shall be sentenced to imprisonment for a maximum of 10 years and/or a maximum fine of Rp.10,000,000,000,-
f. Article 50 of the ITE Law; any person who illegally manufactures and/or distributes computer hardware or software shall be sentenced to imprisonment for a maximum of 10 years and/or a fine of Rp. 10,000,000,-
g. Article 51 of the ITE Law; every person who manipulates the electronic system and commits acts prohibited by the ITE Law and causes losses to others is threatened with imprisonment for a maximum of 12 years and/or a maximum fine of Rp. 12,000,000,000,-.

**Criminal Code (KUHP)**

In an effort to handle the cases that occurred, the investigators made analogies or parables and similarities to the articles in the Criminal Code. Articles in the Criminal Code are usually used more than one article because they involve several acts at the same time articles that can be imposed in the Criminal Code on cybercrime, including:

a. Article 362 of the Criminal Code imposed on carding cases where the perpetrator steals another person's credit card number even though it is not physically because only the card number is the law has existed since 2000 and the last revision of the draft law on criminal acts in the field of information technology since 2004 has been sent to the State Secretariat of the Republic of Indonesia by the Ministry of Communication and Information and sent to the House of Representatives but returned to the Department of Communication and Information to be improved. However, there are several other positive laws that are generally applicable and can be imposed on cybercrime perpetrators, especially for cases that use computers as a means, including: Criminal Code
b. Article 378 of the Criminal Code can be charged for fraud by pretending to offer and sell a product or goods by placing an advertisement on one of the websites so that people are interested in buying it and then sending money to the advertiser. But, in reality, the item does not exist. This was known after the money was sent and the ordered goods did not arrive so that the buyer became deceived.
c. Article 335 of the Criminal Code can be imposed for cases of threats and extortion carried out through e-mail sent by the perpetrator to force the victim to do something according to what the perpetrator wants and if not implemented it will have a dangerous impact. This is usually done because the perpetrator usually knows the victim's secret.
d. Article 311 of the Criminal Code can be imposed for defamation cases using Internet media. The modus operandi is that the perpetrator spreads an email to the victim's friends about a story that is not true or sends an email to a mailing list so that many people know the story.
e. Article 303 of the Criminal Code can be imposed to ensnare gambling games that are carried out online on the Internet with organizers from Indonesia.
f. Article 282 of the Criminal Code can be imposed for the dissemination of pornography and pornographic websites that are widely circulated and easily accessible on the Internet. Even though it is in Indonesian, it is very difficult to take action against the perpetrators because they register the domain outside the country where pornography featuring adults is not illegal.
g. Articles 282 and 311 of the Criminal Code can be imposed on the case of distributing a person's personal photo or film that is vulgar on the Internet.

h. Articles 378 and 262 of the Criminal Code can be applied to carding cases, because the perpetrator commits fraud as if he wants to buy an item and pays with his credit card whose credit card number is stolen.
i. Article 406 of the Criminal Code can be applied to cases of deface or hacking that makes someone else's system, such as a website or program, malfunction or can be used as it should.

**Law No. 28 of 2014 Concerning Copyright**

According to Article 1 number (9) of Law No. 28 of 2014 concerning Copyright, a Computer Program is a set of instructions expressed in the form of language, code, schema, or in any form intended for a computer to work to perform a certain function or to achieve a certain result. The copyright for computer programs is valid for 50 years (Article 58 paragraph (3)). The price of computer programs/software that is very expensive for Indonesian citizens is a promising opportunity for business people to duplicate and sell pirated software at a very low price. For example, an anti-virus program for $50 can be purchased for Rp20,000.00. Sales at a very cheap price compared to the original software produce huge profits for the perpetrators because the capital spent is not more than Rp 5,000.00 per piece. The rise of software piracy in Indonesia that seems "understandable" is certainly very detrimental to copyright owners. The act of hijacking the computer program is also a criminal offense as stipulated in Article 117 paragraph (3), namely "Every person who meets the elements as intended in paragraph (2) committed in the form of Piracy shall be sentenced to a maximum of 10 (ten) years in prison and/or a maximum fine of Rp4,000,000,000.00 (four billion rupiah).

**Law No. 36 of 1999 Concerning Telecommunications**

Article 1 number (1) of Law Number 36 of 1999 concerning Telecommunications states that information transmitted, transmitted, and/or received in any form including writing, images, sounds, and signals through cables, optics, radios, or other electromagnetic systems, is considered a form of Telecommunications. According to this definition, the Internet and all its features are a kind of communication tool because it uses electromagnetic systems to send and receive any kind of information, including sound, images, and video. This law allows for punishment for internet abuse that disturbs public or private order. In particular, hackers who breach other people's network systems may be subject to sanctions under Article 22, which states that: Everyone is prohibited from committing unauthorized, illegal, or manipulative acts. This includes access to dedicated networks, telecommunications services, and networks connected to telecommunications networks.

**Law No. 8 of 1997 Concerning Company Documents**

The government seeks to regulate the recognition of microfilm and other media (information storage devices that are not paper and have a level of security that can guarantee the authenticity of documents transferred or changed) with the issuance of Law Number 8 of 1997 dated March 24, 1997 concerning Company Documents. As a legitimate example, consider Compact Disc - Read Only Memory (CD - ROM) and Write - Once - Read - Many (WORM), both regulated by Article 12 of the Act.

**Law No. 8 of 2010 Concerning the Crime of Money Laundering**

Because fraud is one of the types of criminal acts that are included in the crime of money laundering, this law is the most effective way for investigators to collect information about suspects who commit fraud online without having to go through protracted and time-consuming bureaucratic procedures. cash (Paragraph 1 Article 2 Letter r). Without having to comply with the rules of the Banking Law, investigators can request the identity of the suspect and banking information from the bank handling the transfer. Banking identity and information are considered confidential bank information under the Banking Law. Therefore, if the investigator needs access to the information, he must follow the protocol that has been determined, namely in the form of a letter from the Chief of Police to the National Police Chief which is then forwarded to the Governor of Bank Indonesia. To get the data and information needed, this process takes quite a long time. The process in the Money Laundering Law is accelerated because the Regional Police Chief only needs to send a letter to the local Head of Bank Indonesia with a copy to the Governor of Bank Indonesia and the National Police Chief. This speeds up the acquisition of the necessary data and information and facilitates the investigation process against the perpetrators. The bank provides data that includes registration applications, the number of incoming and outgoing accounts, the time and location of transactions, and other details that make it easier for investigators to track down the perpetrators. In accordance with Article 73 letter b, this law also regulates digital or electronic evidence, namely other evidence in the form of data that is spoken, communicated, received, or stored electronically using optical devices or similar devices.

Based on the explanation above, the implementation of regulations in ensnaring cybercrime in identity theft on e-commerce platforms in Indonesia refers to laws that regulate digital crimes, especially Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). In the context of identity theft, the application of this rule pays attention to Article 30 of the ITE Law which regulates illegal access to computer or electronic systems. Identity theft perpetrators can be subject to this article if they illegally access e-commerce systems to steal or use personal data without permission.

In addition, Article 46 of the ITE Law is also an important legal basis in ensnaring cyber crimes of identity theft. This article regulates criminal penalties against those who commit illegal acts in terms of illegal access and electronic data collection. With Article 46 of the ITE Law, the authorities have a strong legal basis to crack down on identity theft perpetrators on e-commerce platforms.

In addition to the ITE Law, the application of the rules can also involve relevant articles in the Criminal Code (KUHP), although its application may not be directly in accordance with cyber crime cases. In the case of identity theft on e-commerce platforms, the application of Article 362 of the Criminal Code which regulates the theft of goods conventionally may not be appropriate, but the authorities can seek a more relevant legal basis in the ITE Law.

Thus, the application of the rules in ensnaring cyber crimes of identity theft on e-commerce platforms in Indonesia is based on the legal framework listed in the ITE Law, especially Articles 30 and 46, and may involve other

relevant articles according to the case at hand. This aims to ensure effective and fair law enforcement in dealing with cybercrime in today's digital era.

## CONCLUSION AND RECOMMENDATION

The process of investigating the crime of identity theft cybercrime on e-commerce platforms in Indonesia, starting from reporting by the victim or party who feels aggrieved. The initial and most difficult stage is the investigation, where the identification of the source of the data leak is carried out by the cybercrime unit. Enforcement involves surveillance, early detection, and cooperation between authorities and e-commerce platforms to collect digital evidence and catch perpetrators. Obstacles occurred, especially in the arrest and confiscation of evidence. The examination involves an in-depth analysis of crime patterns and the use of a legal framework specific to cybercrime. The completion of the case file ensures justice for the victim and takes action against cybercriminals through appropriate legal processes. Despite facing various obstacles, law enforcement against identity theft cybercrime in e-commerce has become more effective with a deep understanding of information technology and cyber law.

From the results of the study, it can be concluded that the application of rules in ensnaring cyber crimes in identity theft on e-commerce platforms in Indonesia involves several relevant laws, such as the Information and Electronic Transactions Law (UU ITE), the Criminal Code (KUHP), the Copyright Law, the Telecommunications Law, the Corporate Documents Law, and the Money Laundering Crime Law. The law provides a legal basis for law enforcement to handle cases of digital identity theft by imposing criminal sanctions on specific perpetrators of cybercrimes. In addition, the law also regulates digital evidence, facilitating the investigation process against the perpetrators. This shows the commitment of the Indonesian government to protect the public from the threat of cybercrime and strengthen law enforcement in the digital realm.

## REFERENCES

Agus, A. A., & Riskawati, R. (2016). Handling Cyber Crime Cases in Makassar City (Study at the Makassar Kota Besar Resort Police Office). SUPREMACY: Journal of Thought, Research in the Social Sciences, Law and Its Teaching, 11(1), 20–29. https://doi.org/10.26858/supremasi.v11i1.3023

Antoni, A. (2018). Cyber Crime in Online Reading. Conscience: Journal of Sharia and Community Studies, 17(2), 261–274. https://doi.org/10.19109/nurani.v17i2.1192

Cassim, F. (2015). Protecting Personal Information In The Era Of Identity Theft: Just How Safe Is Our Personal Information From Identity Thieves? Potchefstroom Electronic Law Journal (PELJ), 18(2), 69–110. https://doi.org/10.4314/PELJ.V18I2.02

Dewata, M. F. N., & Achmad, Y. (2017). Dualism of Normative and Empirical Legal Research. Yogyakarta: Student Library.

Fadli, M., Widijowati, D., & Andayani, D. (2024). Phishing Cybercrime as reviewed in Criminology Perspectives. Co-Value Journal of Cooperative

Economics and Entrepreneurship, 14(12), 824–835. https://doi.org/10.59188/covalue.v14i11.4335

Habibi, M. R., & Liviani, I. (2020). Information Technology Crime (Cyber Crime) and Its Countermeasures in the Indonesian Legal System. Al-Qanun: Journal of Islamic Thought and Reform, 23(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hartanti, D. N., Titahelu, J. A. S., & Taufik, I. (2021). Application of Criminal Sanctions for Perpetrators of the Crime of Embezzlement of Cash On Delivery Money in Court Decision Number: 139/Pid.B/2020/PN.Amb. TATOHI Journal of Legal Sciences, 1(2), 110–124. https://doi.org/10.47268/tatohi.v1i2.553

Kamran, M., & Maskun, M. (2021). Fraud in Online Trading: A Telematics Legal Perspective. Balobe Law Journal, 1(1), 41–56. https://doi.org/10.47268/balobe.v1i1.501

Malalangi, H. E. (2022). Criminal Liability of Perpetrators of Credit Card Break-ins with Carding Mode According to the Information and Electronic Transactions Law. Lex Crimen, 11(3), 1–12.

Putri, M. A. A. (2020). Bank's Responsibility to Third Parties Who Change Internet Banking PIN and Transfer Customer Funds Reviewed from Banking Law. Al Qodiri : Journal of Education, Social and Religion, 18(1), 39–56.

Saputra, C. D. (2023). Legal Aspects of Telematics in Personal Data Protection. Journal of Legal Certainty and Justice, 5(1), 54–74. https://doi.org/10.32502/khk.v5i1.7968

Sari, I. (2014). The difference between forms of crime that are categorized as cyber crime and cyber warfare. Journal of Information Systems, Suryadarma University, 10(1), 241–260. https://doi.org/10.35968/jsi.v10i1.1002

Sartika, R., Siregar, S. A. I., & Kartika Sari, N. P. R. (2020). Specificity of the Cyber Crime Investigation Process. Journal of Actual Justice, 5(1), 38–55. https://doi.org/10.47329/aktualjustice.v5i1.519

Widodo. (2013). Criminal Law in the Field of Information Technology Cybercrime Law: Theoretical Analysis and Case Analysis. Yogyakarta: Aswaja Pressindo.

Wittadarma, I. G. P. B. P., Sugiartha, I. N. G., & Widyantara, I. M. M. (2022). Juridical Study of the Panel of Judges' Consideration of the Crime of Trademark Counterfeiting (Case Study of the Decision of the District Court. Denpasar No.1080/PID. SUS/2019/PN DPS). Journal of Legal Preference, 3(3), 531–536. https://doi.org/10.55637/jph.3.3.5592.531-536