JILPR Vol. 7, No. 2 February 2026
Journal of Indonesia Law & Policy Review 2715-498X

LAW ENFORCEMENT IN ONLINE FRAUD CRIMINAL CASES IN THE JURISDICTION OF THE POLICE PEKANBARU CITY RESORTS

Muhammad Isnaini[1*], Yeni Triana[2], Indra Afrita[3]
[1,2,3]Master of Law, Lancang Kuning University, Pakanbaru, Indonesia
muhammad.isnaini@gmail.com[1*], yeni.triana@gmail.com[2], indra.afrita@gmail.com[3]

Abstract

In reality, online fraud cases are increasingly prevalent within the Pekanbaru City Police Department, necessitating strict law enforcement. The purpose of this study is to analyze law enforcement in online fraud cases within the Pekanbaru City Police Department and to analyze the actions of the police in resolving online fraud cases within the Pekanbaru City Police Department. The method used is sociological legal research. Based on the research results, it is known that law enforcement against online fraud within the Pekanbaru City Police Department has shown progress, but still faces several obstacles. Legally, this crime is regulated in the Criminal Code and Law Number 19 of 2016 on Electronic Information and Transactions, which provides the legal basis for law enforcement officers to prosecute online fraud perpetrators. The Pekanbaru Police have investigated investigations and inquiries using digital technology, including tracking electronic transactions and identifying the perpetrators' social media accounts. Furthermore, law enforcement also prioritizes victim protection through legal assistance and mediation. However, several significant obstacles remain, including: the difficulty of tracing the perpetrators' identities due to the use of anonymous accounts or domiciles outside the jurisdiction, limited apparatus resources in dealing with technological developments, and slow coordination across relevant agencies such as banks and digital platforms. These obstacles can result in delayed legal proceedings, while victims' losses continue to mount. The Pekanbaru Police's actions in handling online fraud cases include prevention, investigation, prosecution, and law enforcement. In prevention, the Police conduct outreach through social media and educational campaigns to raise public awareness of fraudulent methods. During the investigation and inquiry phase, authorities utilize digital forensics, social media account monitoring, electronic transaction analysis, and coordination with relevant agencies. The City Police also detain eligible perpetrators, confiscate digital and physical evidence, and complete case files for trial.

Keywords: Law Enforcement, Crime, Online Fraud

INTRODUCTION

Law enforcement in online fraud cases within the jurisdiction of the Pekanbaru City Police is a highly relevant topic given the current development of technology and digital society. With the rapid growth of internet use in everyday life, online fraud has become increasingly prevalent, causing material and immaterial losses to victims and causing public unrest. The technology employed by fraudsters is highly sophisticated, exploiting digital platforms and social media to deceive victims through various methods, ranging from fictitious investment offers, the sale of counterfeit goods, to fraudulent schemes disguised as prizes or sweepstakes.

Pekanbaru, the capital of Riau Province, with its ever-increasing number of internet users, is one of the areas not immune to the threat of this crime. This situation necessitates strict law enforcement against perpetrators of online fraud. In this context, Law Number 1 of 2024 concerning Electronic Information and Transactions serves as the legal basis that provides a legal umbrella for prosecution against crimes committed through electronic means, including online fraud. The ITE Law plays a crucial role in protecting the public from the misuse of information technology.

Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions in Indonesia provides a legal framework for the use of information technology and electronic transactions, including social media. The responsive legal theory put forward by Philippe Nonet and Philip Selznick emphasizes that law must be responsive to societal needs and able to adapt to social change. Responsive law is flexible, adaptive, and oriented towards the public interest.

Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactionswas born to regulate the increasingly rapid development and advancement of information technology. One impact of this technological development is that it has placed society in a borderless communication space. This has made it increasingly easy for people to receive and disseminate information electronically at any time and from any location.

Online fraudsters are individuals or groups who commit fraud through digital platforms or the internet, with the goal of obtaining illegitimate profits by deceiving victims. This fraud can be carried out using various methods, exploiting technological advances to disguise their identities and malicious intent. Online fraudsters typically use platforms such as websites, messaging apps, social media, email, or even e-commerce platforms to defraud victims.

The Indonesian legal system regulates fraud and cybercrime through various laws and regulations. Article 378 of the Criminal Code explicitly regulates conventional fraud, while in the digital realm, the provisions are contained in Article 27B of Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, as follows:

(1) Any person who intentionally and without authority distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention of unlawfully benefiting themselves or others, forces people with threats of violence to:
   a. giving an item, which is partly or wholly owned by that person or belongs to another person; or
   b. granting debt, making a debt acknowledgement, or writing off receivables.

(2) Any person who intentionally and without authority distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention of unlawfully benefiting themselves or others, with threats of defamation or with threats of revealing secrets, forcing people to:

a. giving an item which partly or wholly belongs to that person or belongs to another person; or
b. granting debt, making a debt acknowledgement, or writing off receivables.

Article 45 paragraph 8 of the Republic of Indonesia Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, that any person who intentionally and without the right to distribute and/or transmit Electronic Information and/or Electronic Documents, with the intention of unlawfully benefiting himself or another person, forcing a person with the threat of violence to: a. give an item, which is partly or wholly owned by that person or another person; or b. give a loan, make a debt acknowledgment, or write off a receivable, as referred to in Article 278 paragraph (11) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah).

In Article 492 of the Republic of Indonesia Law Number 1 of 2023 concerning the Criminal Code, any person who with the intention of unlawfully benefiting himself or another person by using a false name or false position, using trickery or a series of lies, inducing people to hand over goods, giving debt, making a debt acknowledgment, or writing off receivables, shall be punished for fraud, with a maximum imprisonment of 4 (four) years or a maximum fine of category V.

The prohibition in the Republic of Indonesia Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, the Criminal Code, and with the new Criminal Code that in the ITE Law adapts the form of fraud to the digital realm with heavier criminal threats, while the old and new Criminal Codes still focus on conventional fraud. The new Criminal Code updates the wording and fine system to be more in line with modern legal developments.

Online fraud falls under the category of cybercrime, crimes committed through electronic systems. According to Law Number 8 of 1981 concerning Criminal Procedure Code (KUHAP), law enforcement officers are required to act on any public report that meets the elements of a crime. However, in the context of online fraud, the biggest challenge is digital evidence, which requires forensic expertise, cross-sector collaboration, and mastery of information technology by investigators. In this regard, the Police, particularly the Criminal Investigation Unit (Satreskrim) of the Pekanbaru Police, plays a crucial role in conducting investigations, prosecutions, and law enforcement against perpetrators, supported by existing regulations and legal instruments.

Online fraudsters' modus operandi is diverse, ranging from fake investment scams, offering fictitious goods and services, identity fraud, to scams disguised as sweepstakes or prizes. Perpetrators often deceive victims with enticing promises, such as quick profits or extremely low-priced goods, that in reality do not exist.

Perpetrators also have many methods to carry out their online fraud operations, one of which is called a fraudulent modus operandi. There are three common fraudulent methods in online fraud cases:

1. *Phishing*

   *Phishing*Phishing comes from the word "fishing," meaning fishing. Phishing is a practice where perpetrators falsify data on fake websites that look like real ones, with the aim of stealing the identity of others, impersonating companies, institutions, or agencies. Phishing involves creating fake websites and distributing them widely to attract victims. The websites are designed to be as attractive as possible to attract potential victims.
2. *Scamming*

   *Scamming*Scamming is defined as an act of manipulation by an institution or individual to gain the trust of potential victims and achieve success. Scamming methods vary, including: asking for help, love scamming, and others. Love scamming, which is

synonymous with romance scamming, involves destroying the victim's mental state, leading them to believe they have mutual feelings for each other. Love scamming is often carried out by paying extra attention to the potential victim, so they will comply with their partner's wishes. This includes requesting photos of body parts for personal use. The photos are then disseminated and the victim is threatened with money to prevent the photos from being disseminated. However, this is one strategy used by perpetrators to profit.

3. *Social Engineering*

   *Social Engineering*A method of establishing interaction between the perpetrator and potential victim, using psychological manipulation techniques to make the victim appear to be at fault. Perpetrators subtly deceive through chat or phone calls on various platforms. Common social engineering methods used by fraudsters include online transactions, bank contact centers, fraudulent SMS messages, buying and selling, and so on.

Online fraudsters tend to share several characteristics, such as the ability to deceive and exploit victims' lack of knowledge about technology and the digital world. They also often use false identities or pretend to be legitimate and trustworthy entities, such as large corporations, financial institutions, or famous figures, to increase the credibility of their scams.

Online fraudsters come from a variety of backgrounds, from individuals with in-depth technical knowledge of cyberspace to those simply exploiting victims' laxity. Furthermore, online fraudsters can operate alone or in organized groups. They often utilize international networks to commit these crimes, making them often difficult for law enforcement to track or apprehend.

Obstacles to solving online fraud cases in Pekanbaru City are inextricably linked to the increasingly complex dynamics of information technology development. One of the most significant obstacles is when the perpetrators are located outside Pekanbaru City's jurisdiction, even abroad. This situation fragmented the law enforcement process, as investigators must coordinate across regions and countries. Mutual legal assistance mechanisms are not always efficient, while the perpetrators' digital footprints can be easily erased or diverted. This situation demands strong inter-agency cooperation and adequate technical understanding. However, the reality on the ground shows that such coordination often takes a long time, hampering the effectiveness of investigations. Furthermore, budgetary constraints are also a significant issue. Uncovering online fraud requires sophisticated digital forensic tools, electronic transaction tracking systems, and intensive training for investigators. When budgets are insufficient, investigators often work with limited tools and technical support, making it difficult to track perpetrators and secure digital evidence optimally. These limitations result in slow case resolution and a high risk of losing critical data before it can be secured. Another obstacle is the fact that the cybercrime unit at the Pekanbaru Police was only established this year, so its structure and operations are still being adjusted. The new unit needs time to establish work procedures, establish operational standards, and increase human resource capacity. A lack of experience and a shortage of personnel with expertise in cybercrime have resulted in a slower response to public reports. With all these obstacles, uncovering online fraud cases is a serious challenge that requires ongoing institutional support, budgeting, and technical competence.

This trend indicates that digital technology-based crime in Pekanbaru is experiencing a rapid escalation, in line with the rise in internet usage and electronic transactions. This increase also signals a serious challenge for law enforcement in terms of surveillance, digital tracing (cyber tracing), and adaptive law enforcement to new forms of online fraud.

Article 378 of the Criminal Code regulates the crime of fraud in general. This article states that anyone who, with the intent to unlawfully benefit themselves or another person by using deception or a false position, can be punished with a maximum prison sentence of four years. Fraud committed through electronic media is subject to this article, even if the perpetrator uses technology to commit the fraud.

Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE) is the most important legal basis in handling criminal acts of fraud committed through electronic means or the internet. Several articles in the ITE Law that can be applied to criminal acts of online fraud include: Article 28 paragraph (1): Regulates the dissemination of electronic information that can harm others, including fraud committed through electronic media. Article 28 paragraph (2): Regulates criminal acts related to defamation or fraud committed through information technology, whether in the form of writing, images, or audio visuals that can harm others. Article 45A paragraph (1): Regulates the threat of criminal penalties for anyone who disseminates electronic information containing elements of fraud, defamation, or other violations of the law.

RESEARCH METHODS

The legal research conducted is sociological legal research on the application of positive law in society, especially in relation to the titleLaw Enforcement in Online Fraud Crime Cases in the Jurisdiction of the Pekanbaru City Police. The type of research in this study is empirical juridical, which in other words is a type of sociological legal research and can also be called field research, namely studying the applicable legal provisions and what happens in reality in society (Waluyo, 2002). Or in other words, it is a research conducted on the actual situation or real conditions that occur in society with the intention of knowing and finding the facts and data needed, after the required data is collected then it leads to problem identification which ultimately leads to problem solving (Waluyo, 2002).

The research approach used in this study is a statutory approach, a legal research method conducted by examining and understanding all laws and regulations relevant to the legal issue being studied. This approach positions law as a normative system containing commands, prohibitions, and permits that regulate human behavior in social life, relating toLaw Enforcement in Online Fraud Crime Cases in the Jurisdiction of the Pekanbaru City Police.

A conceptual approach is used to understand legal concepts relevant to the research issue. This approach typically draws on the views of legal experts, legal doctrines, legal theories, and accepted legal principles in legal science.According to Johnny Ibrahim, a conceptual approach is taken because often a law does not explicitly define certain terms or principles, so that the theories and opinions of legal experts become references to clarify them (Ibrahim, 2018).

The analytical approach is an approach that emphasizes the activity of analyzing legal norms, concepts, and principles to find clarity of meaning, relationships between norms, and their legal implications for a concrete event. According to Soerjono Soekanto, legal analysis functions to assess the extent to which the law applies effectively in society, as well as how social, economic, and technological factors influence its application.(Ibrahim, 2018).

The data sources in this study are divided into three categories, namely primary data, secondary data, and tertiary data. Primary data is the main data obtained directly from the first source that has a close relationship with the research problem. Primary data collection was carried out through field activities by conducting direct interviews with law enforcement officers and relevant parties, including the Head of the Criminal Investigation Unit of the Pekanbaru Police, the Head of the Criminal Investigation Unit of the Pekanbaru Police, members of the Criminal Investigation Unit of the Pekanbaru Police, and community leaders.

This primary data serves to describe the factual empirical conditions regarding law enforcement in online fraud cases in the jurisdiction of the Pekanbaru City Police.

In addition to primary data, this study also utilizes secondary data as supporting data obtained through literature review. Secondary data comes from various relevant legal and non-legal sources, such as scientific books, previous research results, official reports, documents, and other literature related to the research object. Secondary data plays a crucial role in providing a theoretical and conceptual foundation, while also strengthening the analysis of primary data obtained in the field. Tertiary data, sourced from legal dictionaries, encyclopedias, and other similar sources, is used as a complement, helping to explain the terms, concepts, and definitions used in the study.

The data collection technique in this study was carried out with the aim of obtaining accurate, valid, and scientifically accountable data. Data collection was adapted to the sociological legal research approach used, thus combining empirical data and library data. Primary data was collected through direct interviews with sources related to the research problem, in order to obtain in-depth and authentic information. In addition, observations were also conducted by carefully observing law enforcement practices in online fraud cases within the jurisdiction of the Pekanbaru Police. To complete the data, the researcher conducted a document study or library study by reviewing various literature and documents relevant to the research topic.

The data collected from various sources is then analyzed using qualitative analysis methods. In sociological legal research, data analysis is not always conducted using a quantitative approach, but rather emphasizes understanding the meaning, patterns, and relationships between data. Therefore, qualitative analysis is conducted by describing and interpreting data in narrative form or systematic and logical sentence descriptions, without the use of statistical figures or mathematical calculations. This analysis aims to provide a comprehensive picture of the problem being studied.

The conclusions drawn in this study were drawn using an inductive method. This method involves drawing conclusions based on specific facts and findings obtained from field research. These facts are then analyzed to identify similarities, patterns, and specific characteristics, allowing for the formulation of a general conclusion that reflects the state of law enforcement in online fraud cases within the jurisdiction of the Pekanbaru City Police.

RESULT AND DISCUSSION

A. Law Enforcement in Online Fraud Cases in the Jurisdiction of the Pekanbaru City Police Department

The development of information and communication technology has brought about significant changes in social interactions and economic transactions. One significant impact of this technological advancement is the emergence of cybercrime, including online fraud. Online fraud is a crime committed through electronic media, whether in the form of the internet, applications, or social media, with the intention of obtaining unlawful gain from the victim through manipulation or deception.(Waluyo, 2021). This phenomenon not only causes material losses for victims but also creates unrest and reduces the sense of security in the community. In Pekanbaru City, as in other cities across Indonesia, online fraud is becoming increasingly prevalent along with the increasing use of digital platforms for buying and selling transactions, investments, and technology-based financial services.

The phenomenon of online fraud in Pekanbaru in recent years has shown a consistent upward trend, particularly through fictitious buying and selling schemes, phishing, lottery scams, banking app manipulation, and even fraud disguised as investments. Empirically, investigators within the Pekanbaru City Police Department face a significantly different complexity compared to conventional forms of fraud. The development of digital technology,

the use of Internet Protocol (IP) masking, anonymous social media accounts, and digitized financial transactions have shifted the scope of investigations toward a highly technical direction, requiring specialized expertise. It is at this point that Law Number 1 of 2024 concerning Electronic Information and Transactions plays a fundamental role as a legal instrument that strengthens the law enforcement framework, making it more relevant to modern forms of cybercrime.

In the empirical context of Pekanbaru, investigators from the Pekanbaru Police Criminal Investigation Unit frequently encounter public reports that essentially describe two major patterns of online fraud: fraud using a social engineering approach and fraud based on platform-based fraud. In the first case, perpetrators exploit victims' psychological weaknesses through communication manipulation, for example by sending One-Time Password (OTP) links, requesting account verification, or impersonating certain parties known to the victim. Meanwhile, the second pattern often uses fictitious advertisements through social media such as Facebook Marketplace, WhatsApp Business, Instagram Shop, and other digital platforms. At the operational level, investigators reported that the majority of incoming cases are dominated by perpetrators located outside Pekanbaru, with most even coming from across provinces, making cross-regional coordination mechanisms a primary need. This fact indicates that online fraud is no longer local, but cross-network and loosely organized.

From a legal perspective, Law Number 1 of 2024 concerning Electronic Information and Transactions provides clearer provisions for criminalizing fraud committed through electronic means. The relevant articles not only contain the element of "unlawful acts" in the context of electronic information distribution but also expand the scope of criminal liability for perpetrators who misuse electronic systems, manipulate transaction data, or disseminate false information that causes harm. While online fraud remains closely linked to Article 378 of the Criminal Code, the enactment of Law Number 1 of 2024 concerning Electronic Information and Transactions provides a lex specialis that allows for prosecution under cyber crime provisions. In the author's opinion, the relationship between the Criminal Code and the updated ITE Law demonstrates a normative dualism mechanism that actually strengthens the evidentiary process because investigators can choose the article with the formulation that best suits the structure of the crime.

Law enforcement against online fraud perpetrators by the Pekanbaru Police must be considered in the context of law enforcement which not only emphasizes the repressive aspect, but also the elements of deterrence and prevention.(Muladi & Arief, 2010). The social reality in Pekanbaru shows that the massive penetration of digital technology has not been accompanied by increased public legal awareness. This is evident in the large number of social media users who readily provide personal data, access unverified links, and conduct transactions without due diligence procedures. Investigators often find that victims only realize they have been defrauded after their money is transferred to an account not in the name of a known party, or after the goods promised by the fictitious seller are not delivered. In fact, this type of crime pattern can actually be prevented with adequate digital literacy. In the author's view, law enforcement should ideally place public education as an integral part of the police strategy in handling technology-based crimes.

The Pekanbaru Police Department's handling of online fraud cases generally begins with a police report, followed by witness examinations, electronic transaction investigations, bank account tracking, phone number and IP address tracking, and data requests from specific electronic system providers. However, investigators acknowledge that technical obstacles often arise, particularly when perpetrators use dummy accounts, burner phone numbers, or payment methods via digital wallets that have been transferred to other parties. Many perpetrators utilize money mules, or holding accounts belonging to others they recruit, to withdraw the proceeds of crime. This situation complicates the process of following the

money because the flow of funds is difficult to trace linearly. Some cases even show perpetrators directly transferring funds to online gambling platforms or illegal crypto exchanges, thereby breaking the digital trail.

Law Number 1 of 2024 concerning Electronic Information and Transactions actually provides a legal basis for investigators to access information from electronic system providers, including telecommunications operators, social media applications, and digital financial institutions. However, according to empirical experience shared by several investigators, data request mechanisms are often hampered by lengthy administrative procedures and differences in data security standards applied by international platforms. This poses a serious obstacle for investigators working under tight deadlines, as some digital evidence is volatile. In many cases, perpetrators who become aware that their identity is being tracked will delete accounts, change phone numbers, or even destroy their devices. These obstacles demonstrate that robust legal instruments have not been fully accompanied by adequate technical readiness and institutional coordination.

From the perspective of law enforcement theory according to Lawrence M. Friedman, the effectiveness of online fraud investigations is influenced by three main elements: legal substance, legal structure, and legal culture. In the Pekanbaru context, the legal substance stipulated in Law Number 1 of 2024 concerning Electronic Information and Transactions and the Criminal Code is actually quite adequate. The legal structure, namely the police institution, specifically the Cyber Crime Unit under the Pekanbaru Police Criminal Investigation Unit, already has relatively competent human resources in digital investigations. However, structural challenges remain because not all investigators have the same cyberforensics skills, and optimal digital forensic equipment is not yet available at the Police level. The final aspect, legal culture, shows that society still has a low digital legal culture, making it very easy for online fraud to develop. If these three elements are not balanced, law enforcement will tend to be reactive and unable to achieve long-term effects.

In several cases handled by the Pekanbaru Police, it is often found that the perpetrators are located outside the jurisdiction or are part of a fraud network operating in a structured manner within a specific region. In such circumstances, Pekanbaru Police investigators must coordinate with other regional police departments through a cross-regional investigative assistance mechanism. This coordination is time-consuming and often hampered by differing perceptions of the urgency of the case. This suggests that a cybercrime-based law enforcement system must strengthen the coordination network between regional police departments throughout Indonesia. In the author's view, modern cybercrime should be handled with a more integrated command structure, similar to a national cyber task force, rather than relying solely on conventional inter-unit coordination.

From an evidentiary perspective, online fraud crimes essentially require investigators to prove the existence of lies, deception, or a series of lies perpetrated electronically. Evidence presented can include screenshots of communications, conversation recordings, transfer receipts, device metadata, and even electronic system activity logs. Challenges arise when victims don't retain complete evidence or only have fragments of edited or partially deleted conversations. Investigators often need to conduct digital recovery to obtain additional evidence. However, in practice, limited forensic equipment makes this process not always feasible. On the other hand, cybercriminals are generally quite skilled at eliminating digital footprints. They use messaging apps with auto-delete features, activate privacy protection, and even hide their locations with VPNs. This situation places investigators in a position where the success of a case depends heavily on the speed of initial action taken on public reports.

Based on field facts, the Pekanbaru Police have taken various strategic steps to strengthen enforcement, such as improving the technical capabilities of investigators through

cyber investigation training, building collaborations with banks, and opening digital reporting channels through the official police application. However, this approach needs to be expanded by establishing a nationally integrated digital crime database so that all police stations can share information with each other to map the perpetrators' networks. The author believes that this integrated system is important because online fraud perpetrators generally commit repeated crimes with the same patterns, only using different accounts, phone numbers, and accounts.

From the perspective of deterrence theory, providing a deterrent effect to perpetrators of crime is very dependent on the consistency of law enforcement.(Rahardjo, 1988). However, in the social reality of Pekanbaru society, many online fraud cases are ultimately dismissed because the victim is reluctant to pursue the case, the perpetrator returns part of the loss, or the family desires a peaceful resolution. The Pekanbaru Police certainly cannot force victims to pursue the case, but this phenomenon causes law enforcement to lose its function as a crime prevention tool. In the author's opinion, peaceful resolution in cybercrime should only be a last resort, especially if the perpetrator is not a repeat offender and the losses are not too large. If the perpetrator is part of a wider criminal network, then a peaceful resolution will only harm the public interest and encourage an increase in crime rates. Therefore, it is necessary to examine the possibility of limiting the space for restorative justice in cybercrime that is detrimental to many parties or has the potential to damage public trust in digital transactions.

Law Number 1 of 2024 concerning Electronic Information and Transactions has attempted to align legal norms with forms of digital crime. The refinement of the definition of electronic systems, the affirmation of norms regarding electronic transactions, and the addition of criminal aspects regarding the misuse of personal data demonstrate the legislators' orientation to keep pace with technological developments. However, the author argues that positive law will only be effective if supported by adequate institutional capacity. Online fraud is not simply an unlawful act committed through electronic means, but rather a criminal structure that exploits society's unpreparedness to enter the digital era. Therefore, the success of law enforcement in Pekanbaru is determined not only by the ability of investigators to apprehend perpetrators, but also by the success of officials in shaping the community's digital legal culture.

The people of Pekanbaru need to be encouraged to understand that digital space is not a safe space. As people become more active in electronic transactions, the risk of data exploitation and manipulation increases.(Soekanto, 2010). Law enforcement officers must play a role not only as enforcers, but also as educators. The Pekanbaru Police Cyber Crime Unit can conduct regular outreach programs, whether through schools, campuses, companies, or digital communities. Digital literacy programs must be made more concrete and based on real cases so that the public understands emerging crime patterns. In the author's view, the public's ability to recognize the signs of online fraud is a key bulwark that will significantly reduce the burden on the police.

As a reflective conclusion, it can be said that law enforcement against online fraud crimes in the jurisdiction of the Pekanbaru Police, based on Law Number 1 of 2024 concerning Electronic Information and Transactions, demonstrates complex dynamics. The law provides a strong legal basis, but its effectiveness depends heavily on structural and cultural readiness. Investigators require technological support, clear authority, and rapid data access. The public needs knowledge to avoid becoming victims. From the perspective of responsive legal theory, law enforcement must be adaptive and progressive. The law must not lag behind the pace of digital innovation. Therefore, authorities, the public, and the state must work together to create a safe and trustworthy digital ecosystem.

Within the positive legal framework, the crime of online fraud is specifically regulated

in the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE) Number 19 of 2016 as an amendment to Law Number 11 of 2008. Article 378 of the Criminal Code states that anyone who, with the intention of unlawfully benefiting themselves or others, by deception, incites others to commit harmful acts, is threatened with a maximum prison sentence of four years. Meanwhile, Article 28 Paragraph (1) of the ITE Law states that anyone who intentionally and without the right to disseminate misleading electronic information and results in consumer losses can be punished with imprisonment and/or a fine. The existence of this regulation shows that the law in Indonesia has adapted to technological developments, but its implementation in the field still faces various obstacles.

Law enforcement against online fraud crimes within the Pekanbaru Police jurisdiction faces both technical and non-technical challenges. Technically, online fraud investigations require specialized skills in cyberforensics, digital data collection, and the ability to track electronic transactions across regions and countries. This is hampered by the limited human resources with these competencies within the regional police.(Soekanto, 2014). Furthermore, electronic evidence is often easily manipulated, difficult to verify, or stored on overseas servers, thus slowing down the investigation and evidence-based process in court (Subekti, 2020).

From a non-technical perspective, public legal awareness also impacts the effectiveness of law enforcement. Many online fraud victims are reluctant to report crimes because they perceive their financial losses to be small or because they don't trust the legal process to resolve the case quickly. This situation makes it difficult for police to collect data and establish crime patterns, making prevention and enforcement efforts less effective.(Hadjon, 2018). Another factor is the relatively new and dynamic nature of regulations; some fraudulent practices evolve faster than existing laws can be refined. This requires law enforcement officials to continually update their knowledge, strategies, and collaborate across agencies, including with banking institutions and e-commerce service providers.

The Pekanbaru Police, as the institution responsible for security in its region, has taken various measures to enforce the law on online fraud. Cases are handled through the stages of police reporting, investigation, and prosecution in court. Police officers utilize digital evidence obtained from telecommunications, bank accounts, and digital platforms to strengthen the evidence, in accordance with strict chain of custody principles to ensure evidence is admissible in court.(Sofyan, 2022). Furthermore, the Pekanbaru Police are also actively educating the public about the dangers of online fraud and the importance of awareness regarding digital transactions, as part of a preventative approach.

Another effort undertaken is to increase human resource capacity through cybercrime training and collaboration with the National Cyber and Crypto Agency (BSSN), financial institutions, and technology companies. This collaboration allows authorities to more quickly detect fraud patterns, block accounts used for crimes, and follow up on reports more effectively. This approach reflects the modern law enforcement paradigm, which emphasizes not only prosecution but also prevention, victim protection, and cross-sector collaboration.(Asshiddiqie, 2020).

Nevertheless, the effectiveness of law enforcement still requires strengthening, particularly in terms of the legal framework. Some online fraud cases have complex characteristics, such as the use of cryptocurrency, digital-based fraudulent investments, and international scams. This requires harmonization of national law with international law and the ability of authorities to conduct cross-jurisdictional investigations. Furthermore, the need to update the Electronic Information and Transactions Law (ITE) to be more adaptive to the latest technological innovations and clarify the responsibilities of digital platforms for fraudulent content is a crucial aspect to support law enforcement.(Kelsen, 1945).

Law enforcement against online fraud within the Pekanbaru Police jurisdiction has demonstrated significant efforts through strengthening officer capacity, utilizing digital evidence, and public outreach. However, challenges such as limited human resources, complex electronic evidence, and the dynamics of digital crime require continuous innovation in legal policies and law enforcement strategies. Regulatory harmonization, cross-agency collaboration, and legal education for the public are key to creating more effective cybersecurity and preventing increased losses from online fraud.

B. Pekanbaru City Police Actions in Resolving Online Fraud Crimes in the Jurisdiction of the Pekanbaru City Police

Online fraud is a form of cybercrime that is increasingly prevalent in the digital era, particularly in large cities like Pekanbaru. This crime is committed through electronic media with the aim of obtaining illegitimate benefits from victims through manipulation, deception, or identity disguising. This situation causes material and non-material losses to the public, as well as causing anxiety and reducing the sense of security in digital transactions.(Waluyo, 2021). This phenomenon requires the police, particularly the Pekanbaru Police, to take proactive and systematic action to resolve online fraud cases in accordance with applicable laws.

The Pekanbaru Police resolve online fraud cases by implementing an investigative mechanism that refers to the Criminal Code and Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE). The settlement process begins with receiving a public complaint, where the victim or injured party files a police report complete with supporting evidence, including digital evidence, transaction evidence, and communications between the perpetrator and the victim. This stage is crucial because it serves as the legal basis for the police to initiate further investigations. In practice, the Pekanbaru Police pay particular attention to the validity of electronic evidence, given its easily manipulated nature and its frequent storage on cross-border servers.(Subekti, 2020).

After receiving the report, Pekanbaru Police investigators conducted an investigation. This phase included data collection, evidence verification, and analysis of the online fraud's modus operandi. Investigators utilized digital forensics to trace the perpetrator's social media accounts, bank accounts, email addresses, and digital platforms. This process also involved coordinating with banks, e-commerce service providers, and telecommunications service providers to access relevant and legally valid data.(Sofyan, 2022). This approach reflects modern law enforcement efforts, where the use of technology is a crucial component in uncovering cybercrime.

The next stage is the investigation, where Pekanbaru Police investigators determine the suspect based on the evidence gathered. In this case, the chain of custody principle is crucial to ensure the electronic evidence obtained is admissible in court. The Pekanbaru Police also implemented a coordinated approach with the Pekanbaru District Attorney's Office to ensure the prosecution process runs effectively. Strict standard operating procedures in the investigation and handling of digital evidence serve as a legal basis for protecting the victim's rights and ensuring the perpetrator's fair trial.

In addition to formal law enforcement, the Pekanbaru Police also take preventative measures through public education and awareness campaigns regarding the risks of online fraud. Through outreach in local media, social media, and collaboration with digital communities, officers provide understanding of fraudulent practices, how to recognize fraudulent indicators, and procedures for reporting cases. This approach not only reduces potential public losses but also strengthens public participation in supporting law enforcement.(Hadjon, 2018).

The Pekanbaru Police are also actively engaging in cross-sector collaboration to

strengthen the resolution of online fraud. Cooperation with financial institutions, the National Cyber and Cyber Crime Agency (BSSN), and technology companies enables rapid information exchange, the blocking of accounts used for fraud, and more efficient legal action. This collaborative approach aligns with the multi-stakeholder governance paradigm, where handling cybercrime is not solely the responsibility of the police but involves various parties to create a more effective digital security ecosystem.(Asshiddiqie, 2020).

However, the Pekanbaru Police's efforts to resolve online fraud cases still face several obstacles. The complexity of electronic evidence, limited human resources with expertise in cyber forensics, and the ever-evolving modus operandi present real challenges. Some cases require international coordination because the perpetrators or servers are located outside of Indonesian jurisdiction, necessitating international legal mechanisms and legal diplomacy for investigation and prosecution.(Soekanto, 2014). This obstacle shows that law enforcement against cybercrime requires continuous innovation, both in terms of regulations, apparatus capacity, and technological support.

Law enforcement against perpetrators of online fraud within the jurisdiction of the Pekanbaru City Police Department faces various obstacles stemming not only from technical and procedural aspects of the police, but also from social and cultural factors, as well as the ever-changing development of digital crime methods. Regulatory changes through Law Number 1 of 2024 concerning Electronic Information and Transactions provide more specific legal instruments for cybercrime, but its implementation in the field still faces significant obstacles. Furthermore, the nature of online fraud as a borderless crime means that investigative work requires technology, speed, inter-agency collaboration, and adequate investigative capacity, while the actual conditions in the field often do not match these needs.

In a number of cases handled by the Criminal Investigation Unit and the Tipidter Unit of the Pekanbaru Police, online fraudsters often use fake accounts, temporary phone numbers (burner numbers), bank accounts borrowed or purchased from other parties, and Virtual Private Network (VPN) devices that create a disjointed digital footprint and obscure their real location. This causes the digital tracing process to take longer, while victims often demand quick results. In an interview with an investigator in November 2025, the investigator stated that "in more than 60% of online fraud cases, the perpetrator's identity is not immediately known when the report is received, so the initial investigation process can take weeks just to confirm the perpetrator's profile."

Although the Pekanbaru Police Department has a special tipidter unit dedicated to handling cybercrime, cyber forensics facilities at the regional level are still inadequate. Many digital evidence extraction tools still rely on the digital laboratory of the Riau Regional Police or even the Criminal Investigation Unit of the National Police Headquarters. This dependence has resulted in long queues for evidence examination, especially in cases requiring the access of devices such as mobile phones or laptops protected by certain security features, including two-factor authentication or encrypted storage.

Although the ITE Law normatively requires electronic system providers to provide data and access when necessary for investigative purposes, in practice, data requests from the police often take a long time due to internal administrative procedures, including verifying the legality of the request, verifying account identity, and internal bank audits to ensure compliance with personal data protection regulations. In one case the author observed, the bank's process of blocking a fraudster's account took almost a month, resulting in the victim's funds being completely withdrawn by the perpetrator before the blocking action could be carried out.

Many victims come to the police station with only proof of transfer, without screenshots of conversations or the perpetrator's account ID. However, under the Electronic Information and Transactions Law (UU ITE), digital crime evidence relies heavily on electronic

communication records. This situation forces investigators to conduct additional investigations, often requiring victims to re-download conversation histories, which may have been deleted. Victims who are technologically illiterate often provide incomplete or inaccessible data, delaying the process of preparing the Investigation Report (BAP).

Public legal awareness also poses a challenge. Although online fraud has become widespread, many Pekanbaru residents still don't understand the characteristics of digital fraud, and are therefore easily lured by the lure of low prices, lottery prizes, or fictitious online loans. Low digital awareness has led to a dramatic increase in the number of reports, but this is not matched by the police's ability to resolve cases quickly. The increase in cases without increasing investigative resources has led to case capacity overload, resulting in some cases having to wait in the investigation queue. From the perspective of Soerjono Soekanto's law enforcement theory, law enforcement and societal factors converge as obstacles, as the quality of community behavior affects police workload, while police capacity is inadequate to meet increasing community needs.

Many perpetrators are domiciled outside the region, even in other provinces in Indonesia. This situation requires investigators to coordinate across regions through regional police backup mechanisms or joint investigations, which require additional costs, time, and effort. Investigators often have to travel outside the region to secure perpetrators or evidence. In practice, budget and resource constraints often force investigators to prioritize cases deemed to have the potential for significant losses, while cases with smaller losses are not optimally handled.

From a regulatory perspective, although the 2024 ITE Law provides a more modern legal framework, several provisions remain open to multiple interpretations in their implementation, particularly regarding the element of "electronic consumer loss" in the online fraud articles. In discussions with investigators, the author found that debate often arises regarding whether an act constitutes pure fraud (Article 378 of the Criminal Code) or electronic transaction-based fraud (the ITE Law). Therefore, investigators must ensure the appropriateness of the elements of the crime before naming the perpetrator as a suspect. Incorrect application of the article can render the indictment null and void in court.

For a single online fraud case, investigators must compile dozens of pages of police reports, coordinate data requests with service providers, conduct case reviews, and ensure each step meets standard investigative procedures. This administrative burden often reduces investigators' time for digital analysis, which is more crucial in cybercrime cases. As one investigator put it, "cyber cases involve a lot of paper, but what we're really looking for isn't paper, it's digital footprints."

Account holders often claim ignorance of the use of their accounts for criminal activity, requiring investigators to conduct in-depth investigations to prove intent or involvement. This process is often lengthy and generates legal debate over whether account holders can be charged as perpetrators or merely witnesses.

It's also worth noting that the success of law enforcement is greatly influenced by the speed of victim reporting. In many cases, victims delay reporting due to embarrassment or the hope that the perpetrator will return the money. However, delaying reporting can cause the perpetrator's digital footprint to disappear due to deleted messages, deactivated accounts, or inactive phone numbers. This situation poses a serious obstacle for investigators because digital evidence is volatile and can easily be lost if not promptly secured.

Psychological barriers also need to be addressed. Victims of online fraud often experience shock, shame, and fear of being blamed for their negligence. Investigators at the Pekanbaru Police Department stated that many victims are highly emotional when reporting, requiring investigators to spend more time systematically gathering information. This trauma and psychological pressure often prevent victims from providing complete statements. This

barrier is often overlooked in law enforcement theory, yet it significantly impacts the quality of police reports.

Theoretically, law enforcement in the context of digital crime is also linked to Lawrence Friedman's legal system theory, which states that the effectiveness of law enforcement is determined by three elements: legal structure, legal substance, and legal culture. In the context of online fraud in Pekanbaru, each of these three aspects presents obstacles. The legal structure (apparatus and work systems) is hampered by limited cyber forensics facilities and human resources. The legal substance still faces challenges in interpreting norms. Meanwhile, the public's legal culture shows low digital literacy and awareness of rapid reporting. These three obstacles are interconnected and reinforce each other, preventing optimal law enforcement.

Furthermore, the increasing sophistication of crime methods requires investigators to continually update their technical skills. However, formal training provided to investigators at the police precinct level is irregular, and not all officers receive it. Investigators admit that many digital investigation methods are self-taught or learned through sharing experiences with others. This irregular training leads to disparities in skills among investigators, resulting in inconsistent investigation quality.

From the author's perspective, these obstacles are rooted in two main issues: first, the caseload is disproportionate to the police's capacity; second, the complexity of cybercrime, which is evolving far faster than the development of regulations and the technical capabilities of law enforcement officers. The author's findings on the ground indicate that despite the authorities' maximum efforts, the support system remains inadequate. Therefore, law enforcement against online fraud requires comprehensive reform, encompassing facilities, training, coordination systems, and public digital literacy. Without this, online fraudsters will continue to exploit loopholes in the law enforcement system to avoid criminal accountability.

The Pekanbaru Police's actions in resolving online fraud crimes reflect an integrated and adaptive law enforcement effort. The process, from receiving reports through investigations, to prosecution, is conducted with attention to legal and technical aspects, including the use of digital evidence and cross-agency collaboration. A preventative approach through education and outreach is also crucial for raising public awareness of the risks of online fraud. While challenges remain, these efforts demonstrate the Pekanbaru Police's commitment to protecting the public from cybercrime and achieving improved digital security.

CONCLUSIONS

Law enforcement against online fraud crimes within the Pekanbaru Police jurisdiction has shown progress, but still faces several obstacles. Legally, this crime is regulated by the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE) Number 19 of 2016, which provides the legal basis for law enforcement officers to prosecute online fraud perpetrators. The Pekanbaru Police have conducted investigations and inquiries utilizing digital technology, including tracking electronic transactions and identifying perpetrators' social media accounts. Furthermore, law enforcement prioritizes victim protection through legal assistance and mediation. However, several significant obstacles remain, including: the difficulty of tracing the identity of perpetrators due to the use of anonymous accounts or domiciles outside the jurisdiction, limited police resources in dealing with technological developments, and slow coordination across relevant agencies such as banks and digital platforms. These obstacles can result in delayed legal proceedings, while victims' losses continue to accumulate.

The Pekanbaru Police's actions in handling online fraud cases include prevention, investigation, inquiry, and law enforcement. In prevention, the Police conduct outreach through social media and educational campaigns to raise public awareness of fraudulent

methods. During the inquiry and inquiry stages, officers utilize digital forensics, social media account monitoring, electronic transaction analysis, and coordination with relevant agencies. The Police also detain eligible perpetrators, confiscate digital and physical evidence, and complete case files for the trial process. Although these actions have been implemented, obstacles remain, including limited supporting technology, slow responses from digital platforms to data requests, and low levels of digital literacy in the community, resulting in late submission of case reports. Furthermore, the complexity of cross-jurisdictional cases makes coordination between regional police departments crucial.

REFERENCES

Asshiddiqie, J. (2020). Constitution and law enforcement in the digital era. Sinar Grafika.
Hadjon, P. M. (2018). Legal protection for the community. Sinar Grafika.
Ibrahim, J. (2018). Theory and methodology of normative legal research. Bayumedia Publishing.
Kelsen, H. (1945). General theory of law and state. Russell & Russell.
Muladi, & Arief, B. N. (2010). Criminal theories and policies. Alumni.
Rahardjo, S. (1988). Law and social change. Sinar Baru.
Soekanto, S. (2010). Factors influencing law enforcement. RajaGrafindo Persada.
Soekanto, S. (2014). Factors influencing law enforcement. RajaGrafindo Persada.
Soekanto, S. (2019). Factors influencing law enforcement. RajaGrafindo Persada.
Sofyan, E. (2022). Digital forensics and cybercrime investigation. Andi Offset.
Subekti, R. (2020). Criminal law and its evidence in digital cases. Citra Aditya Bakti.
Waluyo, B. (2002). Legal research in practice. Sinar Grafika.
Waluyo, B. (2021). Cyber crime and law enforcement in indonesia. Rajawali Pers.