# Banking Secrecy and Law Enforcement: Challenges in Investigating Online Fraud Involving Customer Data

**Hariyanto, Henry Aspan, Mhd. Azhali Siregar**

**Abstract**

This study aims to analyze the challenges faced by law enforcement authorities in investigating online fraud involving customer data protected under banking secrecy principles and to examine the balance between law enforcement interests and the protection of customer information. This research employs normative legal research using statutory, conceptual, and case approaches. Legal materials are analyzed qualitatively to examine the legal framework governing banking secrecy, personal data protection, investigative authority, and the procedures for obtaining customer information during criminal investigations. The results indicate that banking secrecy may constitute a significant obstacle in investigating online fraud, particularly when investigators require account information, customer identities, transaction records, and other financial data to trace and establish the flow of criminal proceeds. At the same time, disclosure of customer information cannot be conducted arbitrarily because it must comply with applicable legal requirements and procedures. The study concludes that harmonization between investigative interests and banking secrecy is necessary through a clear, limited, proportional, and accountable mechanism for accessing customer data. The implication of this research is the need to strengthen the regulatory framework and institutional coordination among law enforcement authorities, banking institutions, and relevant agencies to facilitate effective online fraud investigations while maintaining the legal protection of customer data and banking confidentiality.

**Keywords:** Banking Secrecy; Law Enforcement; Online Fraud; Customer Data; Criminal Investigation.

Hariyanto[1]
[1]Master of Laws, Universitas Pembangunan Panca Budi, Indonesia
e-mail: harrykengchat88@gmail.com [1]

Henry Aspan, Mhd[2]. Azhali Siregar[3]
e-mail: henryaspan@dosen.pancabudi.ac.id[2], azhalisiregar@dosen.pancabudi.ac.id[3]
2nd International Cofference on the Epicentrum of Economic Global Framework (ICEEGLOF)
Theme: Navigating The Future: Business and Social Paradigms in a Transformative Era.
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

## Introduction

The development of information and communication technology has significantly transformed financial transactions and banking services in Indonesia. Digital banking, electronic payments, mobile banking, and internet-based financial services provide convenience and efficiency for the public, but they also create new opportunities for criminal activities, particularly online fraud. Online fraud may involve the misuse of personal information, unauthorized use of bank accounts, social engineering, manipulation of electronic transactions, and fraudulent transfers. The digital nature of these offenses creates difficulties for law enforcement because evidence is often stored electronically, distributed across different systems, and closely connected to financial information protected by legal obligations of confidentiality.

The investigation of online fraud frequently requires investigators to obtain information concerning the identity of account holders, account numbers, transaction histories, transfer destinations, and the flow of funds. Such information is essential for identifying perpetrators, establishing the relationship between the suspect and the victim, tracing criminal proceeds, and constructing the chronology of the offense. However, banking institutions are subject to legal obligations to maintain the confidentiality of customer information. This creates a legal tension between the investigative interests of law enforcement and the principle of banking secrecy. The issue becomes more complex when customer information is simultaneously regarded as personal data that must receive legal protection.

Banking secrecy constitutes an important principle in maintaining public trust in financial institutions. Customers provide banks with personal and financial information on the expectation that such information will be protected and used in accordance with applicable law. Nevertheless, banking secrecy is not an absolute principle. Indonesian banking law recognizes circumstances in which customer information may be disclosed for specific legal purposes, including law enforcement. Therefore, the central legal issue is not whether banking secrecy should be completely maintained or completely disregarded, but under what conditions, procedures, and limitations customer data may be accessed for criminal investigation purposes.

The legal problem becomes increasingly significant in online fraud cases because the investigation of digital financial crimes depends heavily on transaction-related evidence. Unlike conventional fraud, online fraud may be committed without direct physical interaction between the perpetrator and victim. The perpetrator may use false identities, intermediary accounts, electronic communication platforms, digital wallets, or accounts registered under the names of other individuals. Consequently, transaction data held by banks may constitute critical evidence for reconstructing the criminal event. If access to such data is delayed or obstructed, investigators may experience difficulties in identifying perpetrators and tracing the proceeds of crime.

From the perspective of criminal law enforcement, access to banking information is closely related to the principle of effective investigation. Investigators require sufficient authority to collect evidence and establish the facts of a criminal offense. At the same time, the exercise of investigative authority must comply with the principles of legality, proportionality, accountability, and protection of individual rights. This balance is necessary to prevent the interests of law enforcement from becoming a justification for unrestricted access to private financial information.

The issue is also related to the development of Indonesia's legal system in responding to technological changes. Siregar, Fikri Adrian, and Rambe explain that the development of the Indonesian criminal law system is closely connected to changes in social conditions and the development of legal concepts in response to emerging forms of criminality [1]. Online fraud demonstrates the need for legal institutions to adapt traditional investigative mechanisms to criminal activities that increasingly rely on electronic systems and financial technology.

The protection of customer information must also be considered in the context of personal data protection. Customer information held by banks may contain personal data, including identity, account information, transaction history, and financial activities. Therefore, access to such information for investigative purposes must consider not only banking secrecy but also the principles of lawful processing, purpose limitation, necessity, proportionality, and accountability in personal data protection. The interaction between banking secrecy and personal data protection creates a multilayered legal framework that must be carefully harmonized.

Previous studies have discussed different aspects of law enforcement, banking regulation, and the development of criminal law. Research concerning the development of the Indonesian criminal law system emphasizes the need for criminal law to respond to changes in social and technological conditions [1]. Other legal studies have examined law enforcement authority and the exercise of discretion within the criminal justice system. Aspan, for example, explains that law enforcement discretion must remain within legal boundaries and be exercised with accountability in the criminal justice process [2]. This perspective is relevant to online fraud investigations because investigators must exercise their authority to obtain information while maintaining legal certainty and protecting individual rights.

The state of the art of the present research lies in examining banking secrecy not merely as an obligation imposed upon financial institutions, but as a legal issue situated at the intersection of criminal investigation, customer data protection, and law enforcement effectiveness. Existing discussions frequently examine banking secrecy from the perspective of banking obligations or customer protection, while investigations of online fraud tend to emphasize digital evidence and the identification of perpetrators. There remains a need for a comprehensive legal analysis of how these two dimensions can be reconciled when investigators require confidential banking information to establish online fraud cases.

The research gap is therefore found in the limited analysis of the procedural and substantive barriers faced by investigators when accessing customer banking data in online fraud investigations. The problem is not limited to the existence of banking secrecy but also concerns the legal mechanism for obtaining information, the authority of investigators, the requirements for disclosure, the response of banking institutions, the protection of customers who are not perpetrators, and the evidentiary value of banking information obtained during the investigation.

The scientific novelty of this research is the formulation of a balanced legal access model between banking secrecy and law enforcement interests. The model is based on three principles: legality, proportionality, and accountability. The legality principle requires that access to customer information be based on clear statutory authority and established procedures. The proportionality principle requires that the information requested be relevant and necessary to the investigation and not exceed the legitimate investigative purpose. The accountability

principle requires every disclosure and use of customer information to be traceable, documented, and subject to legal oversight.

This approach positions banking secrecy as a principle that must be maintained while recognizing that it may be subject to lawful limitations in the interests of criminal justice. Consequently, the objective is not to weaken banking secrecy but to establish a mechanism through which confidential customer information can be accessed when genuinely necessary for law enforcement. Such an approach is important to maintain public confidence in the banking system while ensuring that banking secrecy does not become an obstacle to combating financial crimes committed through digital platforms.

Based on these circumstances, the main research problems addressed in this article are: first, what are the legal barriers faced by investigators in obtaining customer banking data in online fraud investigations? Second, how should the legal relationship between banking secrecy and the investigative authority of law enforcement be constructed? Third, what legal mechanism can balance the interests of online fraud investigation with the protection of customer data and banking secrecy?

This research therefore aims to analyze the legal challenges associated with accessing customer banking information in online fraud investigations, examine the relationship between banking secrecy and law enforcement authority, and formulate a legal framework that enables investigators to obtain relevant banking information while maintaining the principles of legality, proportionality, privacy, and accountability. The ultimate objective is to contribute to the development of a more responsive legal framework for combating online financial crime without sacrificing legitimate customer protection.

The significance of this research extends beyond the resolution of individual online fraud cases. An effective legal mechanism for accessing banking information may strengthen evidence-based criminal investigations, accelerate the tracing of illicit financial flows, and improve the recovery of victims' losses. At the same time, clear limitations and safeguards are necessary to prevent the misuse of customer information. Therefore, harmonizing banking secrecy, personal data protection, and law enforcement authority is an important prerequisite for establishing a fair, effective, and accountable legal system for addressing online fraud in the digital banking era.

## Literature Review

### 2.1 Banking Secrecy as a Legal Principle in the Banking System

Banking secrecy is a fundamental principle in the relationship between banks and their customers. The principle requires banks and related parties to protect information concerning customers and their financial circumstances obtained through banking activities. The protection of customer information is important because banking relationships are based on trust. Customers provide banks with personal and financial information with the expectation that such information will not be disclosed arbitrarily to third parties. Therefore, banking secrecy functions not only as an obligation imposed upon banks but also as an instrument for maintaining public confidence in the banking system.

However, banking secrecy cannot be understood as an absolute principle. Indonesian banking regulations recognize certain circumstances in which customer information may be

disclosed for legitimate legal purposes. One of the most important exceptions concerns law enforcement. This creates a legal balance between maintaining customer confidentiality and enabling state authorities to obtain information necessary to investigate criminal offenses. The central issue is therefore the establishment of clear limitations and procedures governing the disclosure of customer information.

In online fraud cases, this principle becomes particularly important because banking information frequently constitutes critical evidence. Information concerning account ownership, transaction history, transfer destinations, and the movement of funds may enable investigators to reconstruct the sequence of events and identify the parties involved. Consequently, banking secrecy must be positioned within a legal framework that protects legitimate customer interests while allowing necessary disclosure for criminal justice purposes.

### 2.2 Online Fraud and the Development of Digital Banking

The development of digital banking has fundamentally changed the manner in which financial transactions are conducted. Digital banking provides convenience, speed, and accessibility, but the same characteristics may also be exploited for criminal activities. Online fraud can involve fraudulent electronic transfers, social engineering, identity misuse, fake digital platforms, account takeover, and other schemes that exploit electronic banking systems.

Aspan, Nasution, and Malikhah explain that the development of digital banking in Indonesia is closely connected with the emergence of a cashless culture and the development of regulations governing digital financial transactions [3]. The increasing use of cashless payment mechanisms demonstrates that banking activities are progressively moving toward digital environments. This transformation creates both opportunities and challenges for the legal system because financial transactions become faster while the identification of perpetrators may become more complicated.

The development of digital banking consequently increases the evidentiary importance of banking transaction data. In conventional fraud cases, evidence may primarily consist of physical documents, direct communications, or testimony. In online fraud, however, electronic transaction records may provide essential information concerning the transfer of funds and the relationship between the perpetrator and victim. Thus, access to banking data becomes an important component of effective criminal investigation.

### 2.3 Criminal Law and the Development of New Forms of Crime

The development of online fraud must be understood within the broader development of criminal law. Siregar, Fikri Adrian, and Rambe explain that the Indonesian criminal law system has developed through a long historical process influenced by various legal concepts and social changes [1]. Criminal law is not static; it must respond to changes in social relations and emerging forms of criminal conduct.

The emergence of technology-based crime demonstrates this dynamic character of criminal law. Online fraud differs from conventional fraud in terms of its method, evidence, perpetrators, and geographical reach. A perpetrator may operate from a different jurisdiction, use a false identity, and transfer the proceeds of crime through several accounts. These characteristics create investigative challenges that may not be adequately addressed through traditional investigative approaches.

Siregar's *Buku Ajar Perbandingan Hukum Pidana* further provides a comparative perspective on the development and implementation of criminal law across different legal

systems [2]. Comparative criminal law demonstrates that legal systems respond differently to criminal conduct, investigative authority, evidence, and individual rights. This perspective is relevant to online fraud because digital crime frequently transcends national borders and may require legal mechanisms capable of addressing cross-border evidence and financial transactions.

The development of criminal law therefore requires a balance between effective law enforcement and protection of individual rights. In the context of banking information, this means that investigative authority should be sufficiently effective to uncover criminal activity while remaining subject to legal safeguards designed to protect privacy and confidential financial information.

**2.4 Customer Data Protection and Banking Information**

Customer banking data has a dual legal character. On the one hand, it constitutes confidential information protected by banking secrecy. On the other hand, much of the information may qualify as personal data and therefore receive protection under personal data protection legislation. This creates a multilayered legal framework governing the collection, processing, disclosure, and use of customer information.

The protection of customer data is particularly important because banking information may reveal highly sensitive aspects of an individual's financial activities. Uncontrolled disclosure may create risks of identity theft, financial loss, discrimination, or other misuse. Therefore, the disclosure of customer data for criminal investigation purposes must have a legitimate legal basis and must be limited to information that is relevant and necessary for the investigation.

The principle of purpose limitation is particularly relevant. Information obtained for an investigation should be used for legitimate law enforcement purposes and should not subsequently be used for unrelated purposes. Similarly, the principle of proportionality requires investigators to obtain only information reasonably necessary to establish the criminal offense. These principles provide safeguards against excessive intrusion into customer privacy.

**2.4 Banking Secrecy and the Authority of Law Enforcement**

The relationship between banking secrecy and law enforcement represents a legal tension between two legitimate interests. Banking secrecy protects customer confidentiality and public trust, whereas law enforcement requires access to relevant information to uncover criminal offenses. Neither interest should automatically prevail without considering the circumstances of the individual case.

In online fraud investigations, investigators may need banking information to establish several elements of the offense. First, the information may assist in identifying the recipient of fraudulent funds. Second, transaction records may establish the chronology of financial transfers. Third, account relationships may reveal connections between different suspects. Fourth, financial records may assist in tracing and recovering proceeds of crime.

The problem arises when investigators cannot obtain such information promptly because of banking secrecy requirements. Procedural delays may provide perpetrators with opportunities to transfer funds to other accounts or withdraw the proceeds. Therefore, an effective legal mechanism is required to ensure that legitimate investigative requests can be processed without unnecessarily weakening banking confidentiality.

**2.5 Digital Transactions, Electronic Evidence, and Cyber Notary**

The increasing digitization of transactions also creates challenges concerning the authenticity and reliability of electronic evidence. Aspan et al. explain the importance of strengthening the concept and implementation of cyber notary in online buying and selling activities as part of the development of legal mechanisms responding to digital transactions [4]. The development of cyber notary demonstrates that the legal system must adapt its mechanisms of authentication, documentation, and verification to increasingly digital commercial activities.

This perspective is relevant to online fraud investigations because electronic transactions require reliable mechanisms for identifying parties and establishing the authenticity of digital records. In banking-related fraud, electronic transaction records may become important evidence, but their evidentiary value depends on their authenticity, integrity, and lawful acquisition.

The concept of cyber notary also illustrates the broader transformation of legal institutions in response to technological development. Traditional legal mechanisms based on physical documents and face-to-face interactions increasingly coexist with electronic systems. Consequently, law enforcement institutions must develop investigative mechanisms that are compatible with digital evidence while maintaining procedural safeguards.

### 2.6 The Principle of Legality in Accessing Customer Information

The principle of legality is fundamental to determining whether investigators may access confidential banking information. The exercise of state authority must be based on a clear legal foundation and conducted according to procedures established by law. Investigators should not rely solely on general investigative authority when requesting information protected by specific confidentiality obligations.

The legality principle ensures that disclosure of customer information is not arbitrary. It establishes requirements concerning the competent authority, the purpose of the request, the type of information that may be disclosed, and the procedure for obtaining such information. Consequently, the existence of a legal exception to banking secrecy does not mean that all banking information becomes freely accessible to law enforcement authorities.

This approach is consistent with the development of criminal law discussed by Siregar et al., which emphasizes the importance of understanding criminal law as a system consisting of substantive, procedural, and institutional dimensions [1]. Effective investigation therefore requires not only substantive criminal provisions but also procedural mechanisms that regulate how evidence and information may legally be obtained.

### 2.7 Proportionality and the Limitation of Investigative Authority

In addition to legality, proportionality is an important principle in resolving the conflict between banking secrecy and criminal investigation. The fact that investigators have a legitimate interest in investigating online fraud does not automatically justify unrestricted access to all customer information.

Proportionality requires a relationship between the information requested and the criminal offense under investigation. For example, where the investigation concerns a specific fraudulent transfer, the request should primarily focus on information necessary to identify the relevant account, transaction, recipient, and movement of funds. Requests that extend unnecessarily to unrelated financial activities may constitute excessive interference with privacy.

The principle also supports the protection of third parties whose accounts or information may become involved in an investigation without those individuals being perpetrators. An

account may be used as an intermediary account or may receive funds without the account holder's knowledge. Therefore, investigators must distinguish between the need to obtain information and the presumption that the account holder is criminally responsible.

### 2.8 Accountability and Law Enforcement Discretion

The exercise of investigative authority also requires accountability. Law enforcement officers may face situations in which they must determine what information is necessary, how urgently it is required, and which legal procedure should be followed. Aspan explains that discretion is an important part of law enforcement but must remain within legal boundaries and be exercised responsibly [5].

In banking-related online fraud investigations, discretion should not become a mechanism for bypassing banking secrecy. Instead, discretionary decisions should remain based on applicable law, documented procedures, and legitimate investigative objectives. Every request for banking information should be traceable and capable of being evaluated to determine whether it was legally justified and proportionate.

Accountability is also important from the perspective of banking institutions. Banks must comply with legitimate law enforcement requests while simultaneously ensuring that customer information is not disclosed to unauthorized parties. Therefore, both investigators and banking institutions require clear procedural standards to prevent errors, unauthorized disclosure, and misuse of customer information.

## Research Methodology

This research employs a normative juridical method (*normative legal research*) to analyze the legal challenges faced by law enforcement authorities in investigating online fraud involving bank customer data protected by banking secrecy. This method is appropriate because the research focuses on legal norms, principles, doctrines, and regulatory mechanisms governing the relationship between banking secrecy, customer data protection, and investigative authority. The research seeks to determine how the existing legal framework can provide an appropriate balance between the interests of criminal law enforcement and the protection of confidential customer information.

The research applies three approaches, namely the statutory approach (*statute approach*), conceptual approach (*conceptual approach*), and case approach (*case approach*). The statutory approach is used to examine legislation governing banking secrecy, criminal investigation, electronic transactions, personal data protection, and online fraud. The conceptual approach is used to analyze the concepts of banking secrecy, customer data protection, law enforcement, electronic evidence, legality, proportionality, and accountability. The case approach is used to examine relevant cases and legal considerations concerning the disclosure and use of banking information in the investigation of online fraud and other financial crimes.

The legal materials consist of primary, secondary, and tertiary legal materials. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, the Criminal Procedure Code, and other relevant regulations concerning banking information and criminal investigations. Secondary legal materials consist of scientific journals, books,

legal research, academic publications, and legal doctrines. Relevant literature includes the works of Siregar, Adrian, and Rambe concerning the development of the Indonesian criminal law system [1], Siregar concerning comparative criminal law [2], Aspan, Nasution, and Malikhah concerning digital banking [3], and Aspan et al. concerning cyber notary and online transactions [4]. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference sources used to clarify legal terminology.

The collection of legal materials is conducted through library research and systematic document analysis. Relevant legislation, judicial decisions, academic literature, and regulatory documents are identified, collected, classified, and examined according to their relevance to the research problems. The legal materials are organized into several categories, namely: (1) banking secrecy; (2) customer data protection; (3) online fraud; (4) investigative authority; (5) electronic evidence; (6) procedures for obtaining banking information; and (7) legal safeguards against misuse of customer data.

The primary research instrument is a normative legal analysis framework. The framework is used to identify the legal basis, limitations, and procedures concerning access to customer banking information. The analysis framework consists of several indicators: (1) the legal status of banking secrecy; (2) the legal status of customer data; (3) the authority of investigators to obtain banking information; (4) requirements for disclosure of confidential banking information; (5) evidentiary relevance of customer transaction data; (6) protection of customers whose data is accessed; and (7) accountability mechanisms for the use of banking information.

The collected legal materials are analyzed using qualitative juridical analysis. The analysis employs grammatical, systematic, conceptual, and teleological interpretation. Grammatical interpretation is used to determine the meaning of relevant statutory provisions. Systematic interpretation is applied to examine the relationship between banking law, criminal procedure, electronic information law, and personal data protection law. Conceptual interpretation is used to clarify the concepts of banking secrecy, investigative authority, privacy, and proportionality. Teleological interpretation is applied to determine the objectives of the regulations, particularly the objectives of protecting customers while ensuring effective criminal law enforcement.

The problem-solving analysis begins by identifying the legal position of banking secrecy in the Indonesian legal system. Banking secrecy is intended to protect customer information and maintain public confidence in banking institutions. However, the principle is subject to legally recognized exceptions, including circumstances in which information is required for law enforcement. Therefore, the analysis focuses on determining the circumstances under which the disclosure of customer information may legally occur and the safeguards that must accompany such disclosure.

The second stage examines the investigative requirements in online fraud cases. Online fraud frequently involves the transfer of funds through bank accounts, intermediary accounts, electronic payment systems, and other financial channels. Investigators may therefore require account identity information, transaction records, transfer histories, and information concerning the movement of suspected criminal proceeds. The research analyzes whether existing legal mechanisms provide investigators with sufficient authority to obtain such information and whether the procedures are sufficiently effective to respond to the characteristics of digital crime.

The third stage analyzes the legal barriers to accessing customer banking data. Such barriers may arise from the principle of banking secrecy, procedural requirements for disclosure, limitations on investigative authority, institutional coordination, and concerns regarding the protection of personal data. The analysis distinguishes between legitimate restrictions intended to protect customer rights and procedural obstacles that may unnecessarily hinder criminal investigations.

The fourth stage examines the principle of legality as the primary limitation on investigative authority. Access to confidential customer information must be based on clear statutory authority and must follow established procedures. The principle of legality ensures that banking secrecy cannot be disregarded solely because investigators consider the information useful. There must be a legitimate legal basis connecting the requested information with the criminal offense being investigated.

The fifth stage applies the principle of proportionality. The research assesses whether the scope of banking information requested by investigators corresponds to the needs of the investigation. Information should be limited to data that is relevant and necessary to establish the offense, identify the perpetrator, trace criminal proceeds, or establish the relationship between the suspect and the victim. This principle prevents investigative authority from developing into unrestricted access to the financial activities of customers.

The sixth stage applies the principle of accountability. Every request, disclosure, and use of customer banking information should be capable of being documented and legally evaluated. Accountability applies both to investigators requesting the information and banking institutions providing it. This principle is necessary to prevent unauthorized disclosure, misuse of information, and unnecessary interference with the privacy of customers.

The research also incorporates the perspective of digital banking development. Aspan, Nasution, and Malikhah demonstrate that the development of digital banking and cashless transactions has transformed the financial environment in Indonesia [3]. This development increases the evidentiary importance of electronic banking records in online fraud investigations. Therefore, the research considers whether the existing legal framework has developed sufficiently to accommodate the speed, volume, and complexity of digital financial transactions.

The development of electronic transactions and cyber notary also provides a supporting perspective. Aspan et al. emphasize the importance of developing legal mechanisms that can respond to online transactions and digital legal relationships [4]. This perspective is relevant because the investigation of online fraud increasingly depends on electronic records. Consequently, the legal system must provide mechanisms that ensure electronic information can be lawfully obtained, authenticated, preserved, and used as evidence.

The research further incorporates a criminal law perspective based on the works of Siregar, Adrian, and Rambe [1] and Siregar [2]. The development of criminal law demonstrates the need to adapt legal mechanisms to changes in forms of criminality and social relations. Online fraud represents such a transformation because the offense may be committed remotely and may involve multiple electronic and financial systems. Therefore, investigative mechanisms must be capable of responding to digital crime without abandoning fundamental principles of criminal justice and individual rights.

The final stage of the problem-solving analysis is the formulation of a balanced legal access model for customer banking information. The model is based on three interconnected principles: legality, proportionality, and accountability. Legality establishes the authority and procedure for accessing information; proportionality limits access to information that is relevant and necessary; and accountability ensures that the request, disclosure, and subsequent use of information can be monitored and justified.

Table 1. Balanced Legal Access Model for Customer Banking Data in Online Fraud Investigations

| Principle | Legal Requirement | Practical Application |
|---|---|---|
| Legality | Access must have a clear legal basis and follow the applicable procedure | Investigators submit requests through legally authorized mechanisms |
| Proportionality | Information obtained must be relevant and necessary | Access is limited to accounts, transactions, and data related to the alleged offense |
| Accountability | Access and use of information must be documented and supervised | Disclosure and subsequent use of data are recorded and subject to legal oversight |
| Data Protection | Customer information must be protected from unauthorized use | Information is used only for legitimate investigative purposes |
| Effectiveness | The mechanism must support timely investigation | Coordination between investigators and banking institutions is strengthened |

Through this methodology, the research seeks to produce an objective legal assessment of the obstacles faced by investigators in obtaining banking information in online fraud cases. The analysis does not position banking secrecy and law enforcement as mutually exclusive interests. Instead, it seeks to establish a legal mechanism through which both interests can be protected simultaneously. The final result is expected to contribute to the development of a regulatory framework that enables effective online fraud investigation while maintaining banking confidentiality, customer data protection, legal certainty, and accountability.

## Results

The results of the normative legal analysis demonstrate that the investigation of online fraud involving bank customer data faces a fundamental legal tension between the need for effective law enforcement and the obligation to maintain banking secrecy. Banking information is frequently essential for identifying the recipient of fraudulent funds, tracing the flow of transactions, determining relationships between accounts, and establishing the financial component of an offense. However, the information is simultaneously protected by banking confidentiality and, in many circumstances, personal data protection principles. The findings indicate that the existence of banking secrecy does not eliminate the authority of law enforcement to obtain relevant information, but it requires investigators to comply with specific legal procedures and limitations.

### 4.1 Banking Customer Data as Essential Evidence in Online Fraud Investigations

The first finding is that banking customer data has a strategic evidentiary position in online fraud investigations. Unlike conventional fraud, online fraud frequently occurs without direct physical contact between perpetrator and victim. Communication may take place through digital platforms, while payment is made through bank transfers or other electronic financial services. Consequently, the transaction trail may constitute one of the most important objective sources of evidence.

Banking records may provide information concerning the identity of the account holder, account number, transaction date, amount transferred, recipient account, transfer history, and movement of funds. Such information can assist investigators in constructing the chronology of the offense and determining whether an account was used as an instrument for committing the crime or as a means of receiving the proceeds.

The importance of financial transaction data is consistent with the development of digital banking in Indonesia. Aspan, Nasution, and Malikhah explain that the development of digital banking and the cashless culture has significantly transformed financial transactions and required corresponding regulatory development [3]. The transformation creates an evidentiary environment in which electronic transaction records increasingly become relevant to criminal investigations.

Therefore, the research finds that the effectiveness of online fraud investigations is substantially influenced by the ability of investigators to obtain reliable banking information through lawful mechanisms. When access to such information is delayed, the investigation may encounter difficulties in identifying perpetrators and tracing funds, particularly where the proceeds are rapidly transferred to multiple accounts.

**1. Banking Secrecy as a Legal Protection and Investigative Limitation**

The second finding concerns the dual position of banking secrecy. On the one hand, banking secrecy provides essential protection for customers and maintains trust in financial institutions. On the other hand, banking secrecy may become a procedural limitation when investigators require customer information to uncover a criminal offense.

The analysis demonstrates that banking secrecy should not be regarded as an absolute prohibition against disclosure. Rather, it functions as the general rule from which legally recognized exceptions may arise. Disclosure for criminal investigation purposes must therefore be based on legal authority, follow the prescribed procedure, and remain connected to a legitimate investigative purpose.

This finding is important because treating banking secrecy as absolute could create an unintended consequence: financial institutions might become legally unable or unwilling to provide information that is essential to uncovering criminal activity. Conversely, treating investigative authority as unlimited could undermine customer privacy and public confidence in the banking system.

The appropriate legal position is therefore a controlled disclosure mechanism. Under this mechanism, banking secrecy remains protected as a fundamental principle, while disclosure is permitted when statutory requirements have been satisfied.

**4.2 Legal Obstacles in Accessing Customer Banking Data**

The research identifies several categories of obstacles in obtaining banking customer information during online fraud investigations. The first is the substantive legal obstacle, namely the existence of confidentiality obligations that restrict banks from freely disclosing

customer information. The second is the procedural obstacle, concerning the requirements that must be fulfilled before information can legally be disclosed. The third is the institutional obstacle, which may arise from differences in understanding, coordination, and communication between investigators and banking institutions.

A further obstacle arises from the increasing complexity of digital financial transactions. An online fraud case may involve several accounts, different banks, electronic wallets, intermediary accounts, and transactions conducted within a very short period. Consequently, investigators may need to obtain information from several financial institutions. Where the process is not sufficiently integrated, the investigation may become slower and the tracing of funds more difficult.

The following table summarizes the principal obstacles identified through the legal analysis.

Table 2. Legal Obstacles in Accessing Banking Customer Data

| No. | Type of Obstacle | Legal/Practical Problem | Impact on Investigation |
|---|---|---|---|
| 1 | Banking secrecy | Customer information is protected from unauthorized disclosure | Investigators cannot obtain information arbitrarily |
| 2 | Procedural requirements | Disclosure must follow legally prescribed mechanisms | May cause delays in urgent investigations |
| 3 | Institutional coordination | Different institutions may have different procedures and requirements | Requests for information may take longer |
| 4 | Digital transaction complexity | Transactions may involve multiple accounts and institutions | Difficulties in tracing the flow of funds |
| 5 | Data protection | Customer information must be protected against misuse | Investigators must limit access to necessary data |
| 6 | Cross-border transactions | Funds may move through foreign institutions or platforms | Domestic investigative authority may be insufficient |

These findings demonstrate that the principal problem is not simply the existence of banking secrecy. Rather, the problem concerns whether the legal system provides an effective, predictable, and timely mechanism through which legitimate investigative requests can obtain necessary information while maintaining customer protection.

### 4.3 Conflict Between Law Enforcement Interests and Customer Data Protection

The fourth finding is the existence of a legal balancing problem between law enforcement effectiveness and customer data protection. Customer information may be essential to an investigation even when the customer whose information is requested is not the perpetrator. For example, a bank account may be used as an intermediary account without the account holder's knowledge or may receive fraudulent funds as a result of manipulation.

Therefore, investigators must distinguish between the need to obtain information and the determination of criminal responsibility. Accessing the information of an account holder does not automatically establish that the person is a perpetrator. This distinction is important to prevent investigative information from being interpreted prematurely as proof of criminal liability.

The findings support the principle that customer data may be accessed for legitimate investigative purposes, but its use must remain limited to the purpose for which it was lawfully obtained. Information unrelated to the alleged offense should not be unnecessarily disseminated or used for other purposes.

### 4.4 Legality as the First Requirement for Access to Banking Information

The research establishes that legality must be the first requirement governing access to customer banking data. Investigative authority must have a clear legal foundation, and the process of obtaining information must comply with applicable statutory procedures. The principle prevents investigators from relying solely on the general assertion that the information is "necessary for investigation."

The requirement for a legal basis is consistent with the development of criminal law as a system in which state authority must be exercised according to established legal norms. Siregar, Adrian, and Rambe emphasize the development of criminal law in Indonesia as a legal system that responds to social developments while maintaining the fundamental structure of criminal justice [1]. This principle becomes increasingly important when criminal investigation involves information protected by privacy and confidentiality obligations.

The research therefore finds that a request for customer banking information should clearly identify the criminal case, investigative purpose, type of information requested, relevant time period, and legal authority supporting the request. Such requirements increase legal certainty for both investigators and banking institutions.

### 4.5 Proportionality in the Disclosure of Customer Data

The second safeguard identified is proportionality. The disclosure of banking information should be limited to information that is relevant and necessary to establish the alleged offense. Proportionality is important because bank accounts contain extensive information concerning a person's financial activities, some of which may have no relationship to the criminal investigation.

For example, if an online fraud investigation concerns a specific transfer made on a particular date, the investigative need may be satisfied through information concerning the relevant account, transaction, recipient, and subsequent movement of the suspected funds. There is no automatic justification for accessing unrelated financial information belonging to the same customer.

The proportionality principle therefore creates a legal boundary between necessary investigative access and excessive intrusion. This finding strengthens the argument that banking secrecy and customer data protection should not be sacrificed in the name of law enforcement effectiveness.

### 4.6 Accountability in the Use of Banking Information

The third safeguard is accountability. The analysis finds that access to customer banking information should be recorded, documented, and capable of subsequent review. Accountability applies to both parties: investigators who request information and banking institutions that disclose it.

Aspan's discussion of law enforcement discretion is relevant to this issue because discretionary authority must remain within legal boundaries and be exercised responsibly [5]. In the context of banking information, discretion should therefore not become an instrument for bypassing established confidentiality procedures. Any investigative request should be

supported by a legitimate purpose and capable of being justified through legal and institutional review.

Accountability also provides protection to banking institutions. When banks receive a properly authorized request from competent authorities, clear documentation of the legal basis and scope of disclosure provides certainty that the institution is acting within the law. This creates reciprocal legal protection for investigators, banks, and customers.

### 4.7 Digital Banking Development and the Increasing Importance of Financial Evidence

The research confirms that the growth of digital banking has changed the nature of financial evidence in criminal investigations. Aspan, Nasution, and Malikhah describe the development of digital banking as part of the transformation toward a cashless culture in Indonesia [3]. As transactions become increasingly electronic, banking records become more important in reconstructing financial events.

This phenomenon has two consequences. First, law enforcement authorities require stronger technological and legal capacity to analyze electronic financial records. Second, banking institutions require standardized mechanisms for responding to lawful requests from investigators. Without both elements, the availability of electronic transaction data does not automatically translate into effective criminal investigation.

The development of cyber notary also demonstrates the broader transformation of legal institutions in response to digital transactions. Aspan et al. emphasize the need to strengthen cyber notary mechanisms in online buying and selling transactions [4]. Although the concept operates in a different legal context, the underlying principle is relevant: legal mechanisms must adapt to digital environments to maintain certainty, authenticity, and accountability.

### 4.8 Comparative Criminal Law Perspective

From the perspective of comparative criminal law, the findings demonstrate that the tension between investigative authority and privacy protection is not unique to Indonesia. Modern criminal justice systems generally face the challenge of enabling authorities to obtain digital and financial evidence while preventing excessive interference with individual rights. Siregar's discussion of comparative criminal law provides a conceptual basis for understanding differences in criminal law systems and their approaches to criminal responsibility and enforcement [2].

This perspective becomes increasingly important because online fraud may have transnational characteristics. A perpetrator may operate in one jurisdiction, use a victim's information in another jurisdiction, and transfer the proceeds through accounts or digital platforms located elsewhere. Accordingly, domestic mechanisms for obtaining banking information may need to be supported by mechanisms for international legal cooperation.

### 4.9 Proposed Legal Solution: Balanced Access to Customer Banking Data

Based on the findings, the research proposes a Balanced Banking Data Access Model. The model does not seek to eliminate banking secrecy but to establish a controlled exception that allows law enforcement to access relevant information when legal requirements are satisfied.

Table 3. Balanced Banking Data Access Model

| Stage | Principle | Required Mechanism | Expected Result |
|---|---|---|---|
| 1 | Legality | Clear statutory authority and formal request | Legal certainty |
| 2 | Relevance | Identification of the information directly related to the offense | Focused investigation |
| 3 | Proportionality | Limitation of data according to investigative necessity | Protection of privacy |
| 4 | Timeliness | Efficient coordination between investigators and banks | Prevention of loss or transfer of criminal proceeds |
| 5 | Accountability | Documentation and monitoring of disclosure | Prevention of misuse |
| 6 | Data security | Restricted access and controlled use of information | Protection of customer data |
| 7 | Evaluation | Review of the legality and necessity of access | Institutional accountability |

The proposed model demonstrates that the legal solution does not lie in choosing between absolute banking secrecy and unrestricted investigative access. Instead, the solution lies in regulated and accountable disclosure. Banking secrecy remains the general principle, while access for law enforcement is recognized as an exception subject to legal requirements.

## Conclusion

This research concludes that banking secrecy represents both an important form of customer protection and a potential legal obstacle to the investigation of online fraud. Customer banking information, including account identity, transaction history, transfer records, and the movement of funds, is often essential for identifying perpetrators, reconstructing the chronology of criminal acts, and tracing the proceeds of crime. However, such information cannot be accessed freely because it is protected by banking secrecy and, in relevant circumstances, personal data protection principles. Therefore, banking secrecy should not be understood as an absolute barrier to law enforcement, but disclosure must be conducted only within the limits and procedures established by law.

The research identifies that the principal obstacles in investigating online fraud involving customer banking data consist of banking confidentiality, procedural requirements, institutional coordination, the complexity of digital financial transactions, data protection obligations, and the potential cross-border nature of online fraud. These obstacles can affect the speed and effectiveness of investigations, particularly when perpetrators rapidly transfer fraudulent funds through multiple accounts or financial institutions. The development of digital banking and a cashless culture has consequently increased the importance of banking transaction data as electronic evidence in criminal investigations [3].

The relationship between banking secrecy and law enforcement must therefore be constructed on the basis of legality, proportionality, and accountability. The principle of legality requires investigators to have clear statutory authority and to follow the prescribed procedure

when requesting customer information. The principle of proportionality requires the information obtained to be relevant and necessary to the investigation and prevents unrestricted access to unrelated financial information. Meanwhile, accountability requires every request, disclosure, and use of customer data to be documented, controlled, and capable of legal review. These principles ensure that investigative authority does not develop into excessive interference with the privacy and rights of customers.

The findings further demonstrate that the development of criminal law must respond to technological transformation. As explained by Siregar, Adrian, and Rambe, the development of the criminal law system is closely related to changes in social conditions and forms of criminality [1]. Similarly, the comparative perspective of criminal law emphasizes the importance of adapting legal mechanisms to contemporary forms of crime while maintaining fundamental principles of criminal justice [2]. Online fraud illustrates the necessity of such adaptation because the offense increasingly relies on electronic communication, digital financial transactions, and complex financial networks.

Based on these findings, this research proposes a Balanced Banking Data Access Model, in which banking secrecy remains the general principle while allowing controlled disclosure for legitimate criminal investigation purposes. The model requires: (1) a clear legal basis; (2) identification of relevant information; (3) proportional limitation of the requested data; (4) an efficient disclosure mechanism; (5) data security and restricted use; and (6) institutional monitoring and accountability. This model is intended to ensure that banking secrecy and law enforcement do not operate as mutually exclusive interests.

The scientific implication of this research is the development of an integrated legal perspective connecting banking secrecy, criminal law, digital banking, electronic evidence, and customer data protection. The research demonstrates that the effectiveness of online fraud investigations cannot depend solely on expanding investigative authority. It must also be accompanied by clear procedural safeguards that establish when, why, and to what extent customer information may be accessed. This approach strengthens the legal certainty of both investigators and banking institutions while protecting customers from unnecessary disclosure of their financial information.

The practical implication is the need for stronger coordination between law enforcement authorities and banking institutions. Standardized procedures for responding to lawful investigative requests, efficient communication mechanisms, and improved investigator capacity in analyzing digital financial evidence are necessary to prevent delays in tracing fraudulent funds. At the same time, banking institutions must maintain appropriate internal safeguards to ensure that customer information is disclosed only to authorized parties and for legitimate purposes.

The development of digital banking and online transactions also requires continuous adaptation of legal institutions. The discussion of digital banking by Aspan, Nasution, and Malikhah [3] and the development of cyber notary mechanisms discussed by Aspan et al. [4] demonstrate that Indonesian law must continuously respond to technological transformation. In the context of criminal law enforcement, this adaptation should include mechanisms capable of securing and obtaining electronic banking evidence without weakening the fundamental principles of confidentiality and data protection.

In conclusion, effective law enforcement against online fraud and the protection of banking secrecy are not contradictory objectives. Both can be achieved through a legally regulated mechanism that balances investigative necessity with customer protection. The findings of this research emphasize that access to banking customer data should be lawful, necessary, proportionate, limited, secure, and accountable. Such a framework can strengthen the investigation and prosecution of online fraud while maintaining public confidence in the banking system.

For future research and regulatory development, further empirical and comparative studies are recommended to examine the implementation of banking data disclosure mechanisms, institutional coordination between investigators and financial institutions, and the handling of cross-border digital financial crimes. Regulatory development should also consider technological advances in digital banking and financial technology so that legal mechanisms remain responsive to emerging forms of online fraud. In this way, the legal system can develop toward a model of effective, rights-oriented, and technologically responsive criminal law enforcement without sacrificing the fundamental protection of banking secrecy and customer data.

## References

[1] M. A. Siregar, R. F. Adrian, and M. J. Rambe, *Menelusuri Perjalanan Lahirnya Konsep Sistem Hukum Pidana dan Hukum Pidana di Indonesia*. Medan, Indonesia: Penerbit Tahta Media, 2023.

[2] M. A. Siregar, *Buku Ajar Perbandingan Hukum Pidana*. Serasi Media Teknologi, 2025.

[3] H. Aspan, A. P. Nasution, and I. Malikhah, "Digital banking in Indonesia: The development of cashless culture and regulations," *International Journal of Research and Review*, vol. 9, no. 1, pp. 534–543, 2022.

[4] H. Aspan *et al.*, "Enhance Cyber Notary for Buyers Online Buying and Sale," *Jurnal Ekonomi*, vol. 12, no. 2, pp. 1684–1688, 2023.

[5] H. Aspan, "Diskresi aparat penegak hukum dalam sistem peradilan pidana," *Jurnal Hukum*, vol. 10, no. 2, pp. 115–128, 2021.

[6] Republic of Indonesia, Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, Jakarta, Indonesia, 1998.

[7] Republic of Indonesia, Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, Jakarta, Indonesia.

[8] Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, Jakarta, Indonesia, 2022.

[9] Republic of Indonesia, Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP), Jakarta, Indonesia, 1981.

[10] Republic of Indonesia, Law Number 1 of 2023 concerning the Criminal Code (KUHP), Jakarta, Indonesia, 2023.

[11] Republic of Indonesia, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Jakarta, Indonesia, 2019.

[12] Republic of Indonesia, Financial Services Authority Regulation concerning the Implementation of Digital Banking Services by Commercial Banks, Jakarta, Indonesia.