

Article

Mule Accounts in Digital Fraud Criminal Liability of Account Holders Between Participation and Money Laundering

Abidi Alif Negara

¹Master of Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia

Article information	Abstract
DOI : xxx Correspondence :	The growth of digital banking, electronic wallets, and internet-based payment systems has expanded access to financial services while creating new opportunities for cyber-economic crime. Because offenders must still cash out the proceeds of digital fraud, they increasingly rely on accounts belonging to other persons—known as mule accounts, to separate criminal proceeds from the identity of the principal offender. By 14 July 2026, the Indonesia Anti-Scam Centre had received 608,167 reports and identified more than one million accounts reportedly connected with fraud. This scale raises a legal problem: holders are not a uniform category, ranging from knowing participants to victims of hacking or identity theft, and formal account ownership alone cannot establish fault. This study examines the legal status of mule-account holders within digital-fraud schemes and the criminal liability they bear for receiving and transferring fraud proceeds under Indonesian money-laundering law. The study is normative legal research employing statutory, conceptual, and hypothetical-case approaches. It analyses the participation provisions of Articles 20 and 21 of Law No. 1 of 2023 (the National Criminal Code), which entered into force on 2 January 2026, together with Article 607 governing money laundering and the provisions of Law No. 8 of 2010 that remain in force, as confirmed by Law No. 1 of 2026. The analysis shows that a holder may be classified as a joint perpetrator where there is close, conscious cooperation from the outset; as an accessory where the holder intentionally supplies banking means without close involvement in execution, carrying a maximum penalty of two-thirds of the principal penalty under Article 21(3); or as not liable for the predicate offence where the account is misused without knowledge or intention. Under Article 607, active money laundering arises from dealings intended to conceal the origin of proceeds, while passive money laundering under Article 607(1)(c) requires only receipt or control of property known or reasonably suspected to be criminal proceeds. Enforcement should prioritise the holder’s factual role and mental state over the name recorded in banking records, allowing knowing facilitators to be held proportionately liable while protecting genuine victims of account misuse.
Submission Track	
Submission : April 10, 2026 Final Review : June 02, 2026 Accepted : June 10, 2026	
Keywords	
crypto-asset investment, cybercrime, criminal liability, economic criminal law, legal certainty	



This is an open access article under the CC BY <https://creativecommons.org/licenses/by/4.0/>

INTRODUCTION

The development of information technology has fundamentally changed the way in which society conducts economic activities. Digital banking services, electronic wallets, and internet-based payment systems enable financial transactions to be completed rapidly without requiring the parties to meet in

person (Chen et al., 2021; Lindman et al., 2017; Sudirman & Disemadi, 2022). On the one hand, these developments increase efficiency and expand public access to financial services. On the other hand, dependence on electronic systems creates new opportunities for criminal offences in which technology is used to obtain unlawful economic gain. In this context, the prevalence of illegal practices such as the sale of bank accounts via e-commerce platforms has significantly facilitated the laundering of proceeds derived from illicit activities including fraud, drug trafficking, and online gambling (Pane et al., 2024).

Information-technology development not only provides benefits but also continuously transforms the forms and methods of crime. Cybercrime differs from conventional crime because it may be committed remotely and across territorial boundaries, while using electronic identities and networks to impede identification of the perpetrator (Anastasia et al., 2019; Martin, 2025). In an economic context, these characteristics appear in various forms of digital fraud, including phishing, bank-account takeover, investment fraud, manipulation of electronic commerce, business email compromise, and social engineering designed to induce victims to disclose information or transfer funds to offenders (Juneja et al., 2024; Schmitt & Fléchais, 2024).

Cyber-economic crime does not end when an offender obtains funds from a victim. The offender must still receive, transfer, withdraw, or convert those funds into a form that can be controlled and used without revealing the identity of the principal perpetrator. In cybercrime literature, this stage is known as the cash-out process: removing criminal proceeds from the system or account directly connected to the victim and transferring them to the party controlling the crime (Custers et al., 2018; Patsakis et al., 2023). This process is critical to the success of cyber-economic crime because the proceeds must be separated from the identity and conduct of the principal perpetrator.

Custers, Pool, and Cornelisse explain that one method of cashing out and disguising the proceeds of digital-banking crime is to route the funds through accounts belonging to other persons (Custers et al., 2018). These accounts may receive funds from victims and then facilitate their immediate withdrawal in cash or transfer through additional accounts. The use of such intermediaries creates a separation between the victim, the principal offender, and the person who ultimately controls the proceeds. It therefore reduces the evidentiary visibility of the original offence and complicates efforts by law-enforcement authorities to reconstruct the transaction chain, identify the principal perpetrator, and establish the connection between the predicate offence and the benefit obtained. The account of another person is consequently not merely a passive receptacle for illicit funds; when knowingly made available for this purpose, it becomes an operational instrument in the cash-out process and in the concealment, movement, and control of criminal proceeds. This distinction is legally significant because the account holder's liability should depend not on formal ownership alone, but on whether the holder knowingly and intentionally contributed to the circulation or concealment of the proceeds.

An account belonging to another person and used to receive, transfer, or otherwise process criminal proceeds is commonly referred to as a mule account, while the person who provides, controls, or operates the account is known as a money mule. A money mule functions as an intermediary between criminal offenders and the legitimate financial system. Depending on the arrangement, the mule may receive or transfer funds, withdraw cash, surrender access to an account, or convert the proceeds into another form of asset. These activities help criminal networks obscure transaction trails, conceal the origin and destination of illicit funds, and create distance between the principal offenders and the proceeds of crime. The mule account therefore serves not merely as a passive channel for receiving money but as a potentially significant instrument in the concealment, movement, and cashing out of criminal proceeds (Custers et al., 2018; Levi & Soudijn, 2020).

Money mules are not a uniform category of offender, and their criminal liability should not be determined solely by the fact that an account is registered in their name. Some account holders knowingly provide access to their accounts in exchange for a commission or other payment, thereby intentionally

facilitating the receipt, transfer, or withdrawal of criminal proceeds. Others are recruited through fraudulent job offers, friendships, romantic relationships, or manipulation and may not understand the full scope of the criminal scheme (Berry et al., 2023; Levi & Soudijn, 2020). The extent and legal significance of a person's involvement may depend on social relationships, economic necessity, the expectation of quick financial gain, the circumstances in which the account was provided, and the person's knowledge of the associated legal risks (Sarkar et al., 2026; Zali & Maulidi, 2018). Accordingly, liability must be assessed by examining the account holder's actual conduct, knowledge, intention, and contribution to the offence. Formal account registration, without evidence that the holder knowingly or negligently facilitated the criminal activity, is insufficient by itself to establish criminal responsibility.

The use of receiving accounts has become increasingly important as reports of digital financial fraud rise in Indonesia. By 14 July 2026, the Indonesia Anti-Scam Centre had received 608,167 reports and identified more than one million accounts reportedly connected with fraud. These data show that bank accounts and digital-payment accounts are important links in technology-enabled financial fraud. The large number of reported accounts, however, does not establish that all account holders knowingly participated in fraud. Each holder's conduct and mental state must still be assessed individually.

A legal problem arises when an account holder claims not to have known that the account was used to receive criminal proceeds. Several forms of involvement are possible. First, the holder may know of the fraud from the outset and deliberately provide the account as part of its execution. Second, the holder may not participate in deceiving the victim but may know, or reasonably ought to suspect, that the received funds are criminal proceeds and nevertheless help transfer or withdraw them. Third, the holder may surrender account access without knowing its intended use, while receiving compensation or disregarding circumstances that should reasonably arouse suspicion. Fourth, the account may be used through identity theft, hacking, or unauthorised access without the holder's knowledge.

These circumstances have different consequences for legal classification and criminal liability. Criminal law examines not merely the resulting harm but also the conduct, fault, knowledge, intention, and mental relationship between the accused and the offence. Criminal liability requires culpable fault attributable to the offender. Formal account ownership cannot therefore be the sole basis of punishment in the absence of proof concerning the holder's participation and fault. This change gives the study of mule accounts both academic and practical importance. The issue concerns not only the possible application of fraud or money-laundering offences but also the boundary between participation in a predicate offence and involvement in managing its proceeds. An account holder may provide an account before the fraud occurs, receive and move money after it occurs, or perform both acts as part of a planned sequence.

This study examines the use of mule accounts in digital fraud and the limits of account-holder liability. It seeks to identify when a holder may be classified as a joint perpetrator or accessory to the predicate offence and when the holder's conduct satisfies the elements of money laundering. It also analyses the relevance of actual knowledge and reasonable suspicion in distinguishing a holder who knowingly facilitates crime from one who is a victim of account misuse. The study therefore addresses the following questions:

1. What is the legal status of a mule-account holder within a digital-fraud scheme under Indonesian criminal-law provisions on participation?
2. What criminal liability does a mule-account holder bear for receiving and transferring proceeds of digital fraud under money-laundering law?

METHODS

Research Design

This study employs a normative legal research methodology (doctrinal legal research) to examine

the legal status and criminal liability of mule-account holders in digital-fraud schemes. The normative approach is utilized to analyze existing legal principles, statutory norms, and the coherence of the legislative framework governing economic crimes and money laundering in Indonesia.

Legal Approaches

- To address the research problems systematically, this study applies three complementary analytical approaches:
- Statutory Approach (*Pendekatan Perundang-undangan*):** Used to examine relevant legislative acts, particularly focusing on:
- Articles 20 and 21 (Participation/ *Deelneming*) and Article 607 (Money Laundering) of Law No. 1 of 2023 (the National Criminal Code / KUHP).
- Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes, including its continuing validity as confirmed by Law No. 1 of 2026.

Sources of Legal Materials

The study relies on legal materials categorized into two primary tiers:

Primary Legal Materials, including:

1. Law No. 1 of 2023 on the Criminal Code (KUHP).
2. Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering.
3. Law No. 1 of 2026 regarding the adjustments/continuation of anti-money laundering provisions.

Secondary Legal Materials , including legal textbooks, peer-reviewed academic journals on cyber-economic crime, official statistics and reports from the Indonesia Anti-Scam Centre (IASC), and legislative commentaries (*Memorie van Toelichting*).

RESULT AND DISCUSSION

Legal Status of a Mule Account Holder in Digital Fraud

Mule Accounts as Instruments of Digital Fraud

A mule account is an account held in one person's name but used by that person or another individual to receive, control, transfer, or withdraw criminal proceeds. The person who knowingly provides or operates the account is commonly described as a money mule (Bekkers et al., 2023). In financially motivated cybercrime, the mule is not merely an incidental intermediary; the mule functions as a critical link between the principal offender and the legitimate financial system. By routing victims' funds through an account that does not belong to the principal offender, the arrangement separates the initial fraudulent transaction from the eventual receipt or cashing out of the proceeds (Anastasia et al., 2019; Levi & Soudijn, 2020). This separation obscures the movement of funds, complicates transaction tracing, facilitates the conversion of digital proceeds into cash or other assets, and may hinder the identification and prosecution of the principal offender. Accordingly, the account may constitute an operational instrument in the execution and concealment of digital fraud, rather than a neutral banking facility. Nevertheless, the account's functional importance does not, by itself, establish the holder's criminal liability; liability depends on proof that the holder knowingly and culpably contributed to the criminal scheme.

Money mules play a critical role in financially motivated cybercrime because they connect the principal offenders to the legitimate financial system and enable the movement and concealment of criminal proceeds (Gundur et al., 2021; Leukfeldt et al., 2016). By receiving, transferring, or withdrawing victims' funds through accounts that are not controlled directly by the principal offenders, they obscure the financial trail and help preserve the offenders' anonymity. Their involvement may therefore extend

beyond that of a passive intermediary: depending on their conduct and state of mind, money mules may perform an operational function in both the execution of the fraud and the subsequent concealment or conversion of its proceeds. Nevertheless, money mules do not possess the same degree of knowledge or involvement. Some knowingly cooperate in the scheme, whereas others are recruited through manipulation, friendship, fraudulent employment opportunities, or promises of quick income. This distinction is legally decisive because the existence of a transaction through a person's account does not, by itself, establish that the account holder intentionally facilitated the offence. Liability must instead be determined by examining the holder's knowledge, intention, conduct, and contribution to the criminal scheme.

Funds move from victims' accounts to money-mule accounts and are then withdrawn through ATMs. In phishing and banking-malware cases, money mules convert digital criminal proceeds into cash, thereby interrupting the financial trail between the victims and the principal offenders (Custers et al., 2018; Gundur et al., 2021; Hülse, 2017). This cash-out function is not merely a post-offence convenience: it is often an essential operational step through which criminal proceeds are made accessible, concealed, and less readily traceable. Although money mules generally occupy the outer layer of a criminal network, their role may be indispensable because principal offenders depend on third-party accounts and the mules' physical acts to complete the conversion of stolen funds into cash (Anastasia et al., 2019; Leukfeldt et al., 2016). Accordingly, an account holder who knowingly supplies the account, monitors incoming transfers, or withdraws the funds may contribute materially to the execution and concealment of the fraud. However, the account's functional importance must be distinguished from the holder's criminal liability: the holder's role supports liability only where it is accompanied by proof of intentional and culpable participation..

A receiving account is therefore not necessarily an incidental object in the commission of an offence. In some circumstances, it is deliberately prepared and made available so that a principal offender can receive, transfer, or withdraw fraud proceeds without exposing the principal's identity or directly linking the proceeds to the fraud. The account may consequently function as an instrument that facilitates both the execution of the fraudulent scheme and the concealment or movement of its proceeds. However, the account's importance within the criminal sequence does not, by itself, make its holder a participant. Criminal liability requires proof that the holder's conduct materially contributed to the offence and that the holder acted with the requisite knowledge and intention. The decisive issue is therefore not merely whether the account was used, but whether the holder knowingly and culpably provided or operated it as part of the criminal scheme..

Participation Under the National Criminal Code

Article 20 of the National Criminal Code establishes several forms of perpetration relevant to the legal classification of a mule-account holder. A person may be punished as a perpetrator where the person commits the offence personally, commits it through an instrument, orders another person who cannot be held responsible to commit it, jointly commits the offence, or induces another person to commit it by the means specified in the provision. Article 21, by contrast, governs accessory liability. It applies where a person intentionally provides an opportunity, means, or information for the commission of an offence, or intentionally assists while the offence is being committed. This distinction is essential: the use of an account in a fraudulent transaction does not automatically make its holder a perpetrator or an accessory. The classification depends on the holder's actual contribution, the closeness of the cooperation, and proof that the holder acted with the requisite knowledge and intention. Thus, the decisive question is not merely whether the account facilitated the movement of criminal proceeds, but whether the holder knowingly participated in the offence as a principal or intentionally assisted its commission as an accessory.

The elucidation of Article 20 provides that joint commission exists where several persons knowingly

and closely cooperate in the physical commission of an offence. Their acts need not be identical, and no participant is required to perform every element of the offence. Instead, the participants' conduct is assessed collectively as a single criminal undertaking. Accordingly, an account holder may qualify as a joint perpetrator even without personally deceiving the victim if the holder knowingly performs an essential part of the agreed plan, such as supplying and controlling the account, monitoring incoming funds, withdrawing the proceeds, or transferring them as directed. The decisive consideration is whether the holder acted pursuant to a common intention and made a coordinated contribution to the execution of the offence.

The principal distinction between joint commission and assistance is therefore the intensity and quality of cooperation. Joint commission requires close and conscious cooperation in carrying out the offence, with the participant's conduct forming part of the common execution of the criminal plan. Assistance, by contrast, involves a less integrated contribution, such as providing an opportunity, means, or information without participating closely in the offence's execution. Thus, the mere fact that a fraud proceeds through an account does not establish joint commission. The classification depends on whether the account holder shared the criminal plan and actively performed a coordinated role in bringing it about, or merely provided intentional but more limited assistance.

The doctrine of participation determines the criminal liability of persons involved in the same offence, even where their acts and levels of involvement differ (Bois-Pedain, 2019; Wells & Quick, 2012). Although the law recognises distinct forms of participation, such as perpetration, joint perpetration, instigation, and accessory assistance, each form requires proof of culpable fault. Liability therefore cannot be inferred merely from a person's formal connection to an account or from the fact that the account was used to receive or transfer criminal proceeds (Alhajeri & Alhashem, 2023). The appearance of a person's name on an account is evidentially relevant, but it cannot substitute for proof that the person knew of the unlawful conduct and intentionally contributed to it. The account holder's liability must instead be determined by examining the holder's actual conduct, degree of cooperation, knowledge, and intention. This distinction is essential because the same account may be used in circumstances giving rise to joint perpetration, accessory liability, or no criminal liability at all.

The status of a mule-account holder may therefore be divided into several categories.

1. Account Holder as a Joint Perpetrator

An account holder may be treated as a joint perpetrator of digital fraud where, from the outset, the holder knowingly and closely cooperates with the principal offender (Anastasia et al., 2019). Such cooperation may be demonstrated where the holder knows of the planned fraud, understands that the account will receive victims' funds, and performs part of the plan. The holder need not personally communicate false statements to a victim. Their assigned role may instead be to monitor incoming funds, confirm receipt to the principal offender, withdraw the money, divide the proceeds, or forward funds to another account. If those acts were planned from the beginning and formed part of executing the offence, all participants' conduct may be regarded as a single whole.

In a hypothetical case, A may be classified as a joint perpetrator if, before the fraud, A knew of B's plan and agreed to a division of tasks. Supplying the account, monitoring transactions, withdrawing funds, and receiving a share of the proceeds demonstrate an active contribution beyond merely providing a facility. Such conscious cooperation may establish a common intention to bring about the offence. Such liability is often anchored in the "knowing" element, where the participant's subjective awareness of the criminal scheme directly dictates their classification as a principal rather than an innocent party (Zhan, 2025). This conclusion would be reinforced by communications concerning targeted victims, transfer times, expected amounts, withdrawal methods, or division of proceeds. Conversely, if A merely surrendered an account without knowing what offence was planned and did not participate in its execution, joint commission would be more difficult to establish.

2. Account Holder as an Accessory

If an account holder knows that the account will be used for an offence but does not cooperate closely in the execution of the fraud, the holder is more appropriately analysed as an accessory (Baker, 2016). Article 21(1)(a) of the Criminal Code expressly covers intentionally providing an opportunity or means to commit an offence. Such accessory liability arises when an individual provides technical, logistical, or financial support—such as granting access to banking or telecommunication services—with the awareness that these resources are instrumental to the commission of a crime, even if their involvement remains detached from the core execution (Huang, 2024; Kupczyński, 2025). A bank account, ATM card, SIM card, PIN, and mobile-banking access may constitute means because they allow the principal offender to receive and control a victim's funds. The means must be provided intentionally: the holder must know that the act facilitates the principal offender's commission of the offence.

It is not enough to prove only that B used A's account. It must be proved that when A surrendered access, A at least knew the account would be used for an offence and intended to provide the assistance. Intention to assist does not necessarily require A to know every victim's identity or every detail of the scheme, but A must be aware of the unlawful nature of the activity being facilitated. If A rents out the account believing B's claim that it will receive payments for a lawful business and no circumstances arouse suspicion, intentional assistance may not be established. The position differs if A surrenders the account to a stranger, receives an unreasonable payment, provides all banking-security instruments, and knows that incoming funds will be withdrawn immediately. Taken together, these circumstances may show that A's claim of ignorance is implausible. In such scenarios, the account holder's willingness to exchange access for financial gain despite the high probability of illicit activity supports a finding of criminal intent (Bulut, 2024).

The Criminal Code also distinguishes the punishment of a perpetrator from that of an accessory. Under Article 21(3), the maximum punishment for an accessory is two-thirds of the maximum principal penalty for the relevant offence. The classification of the account holder must therefore be determined carefully because it directly affects the severity of criminal liability. Moreover, this assessment requires a granular analysis of the subjective element, as the law necessitates evidence that the individual possessed clear awareness of the fraudulent origin of the assets while simultaneously intending to aid the primary offender.

3. Account Holder Who Cannot Be Held Liable

Not every holder of an account that receives fraud proceeds can be punished. An account may be used through identity theft, document forgery, account hacking, SIM-card takeover, or misuse of access by a previously trusted person. In such circumstances, the formal holder neither supplies the means nor intends to assist the offence (Gundur et al., 2021). An account holder may also be manipulated. For example, a person may be recruited through a fraudulent vacancy and asked to receive purported company payments before forwarding them elsewhere. It must then be assessed whether the holder genuinely did not know of the unlawful activity or instead disregarded signs that reasonably indicated criminal conduct. This distinction is increasingly relevant as “droppery” phenomena evolve, where individuals unwittingly facilitate the illicit movement of funds associated with criminal origins, often complicating the evidentiary chain required for prosecution (Zezyulina, 2026).

Negligence or circumstances giving rise to “reasonable suspicion” do not, by themselves, suffice for liability based on participation or assistance. Article 21 requires intentional assistance. A person cannot be deemed an accessory to digital fraud merely because greater caution was expected unless it is proved that the person knew of and intended to facilitate the offence. Consequently, this evidentiary threshold for intent creates a regulatory gap that some jurisdictions attempt to address through the doctrine of dormant responsibility, which holds parties accountable for the omission of duties to prevent foreseeable criminal misuse of their assets (Tambunan & Barthos, 2025). However, such an extension

of liability necessitates a delicate balance between effectively combating cyber-enabled financial crime and upholding individual human rights (Muk, 2025).

The holder's status in the predicate offence therefore depends on the degree of cooperation and intention. The holder may be a joint perpetrator where there is close, conscious cooperation with the principal offender; an accessory where the holder intentionally supplies the means but is not closely involved in execution; or not liable for the predicate offence where the account is used without their knowledge and intention.

Criminal Liability Under Money Laundering Provisions

Fraud as a Predicate Offence

Money laundering concerns the handling of property derived from criminal activity. It is not limited to sophisticated financial schemes; it also encompasses seemingly routine acts, such as receiving, transferring, withdrawing, or converting funds through a bank account, that are intended to conceal or disguise their criminal origin. The process therefore consists of a sequence of transactions designed to distance criminal proceeds from the underlying offence and create the appearance that they derive from lawful activities (Levi & Soudijn, 2020). Accordingly, a mule-account holder may incur money-laundering liability not merely because the account received fraud proceeds, but because the holder knowingly or reasonably suspected their illicit origin and then participated in transactions that preserved, moved, or used those proceeds (Alhajeri & Alhashem, 2023; Gundur et al., 2021). This distinction is essential: receipt alone does not automatically establish money laundering, whereas deliberate control or movement of criminal proceeds may demonstrate the conduct required by the applicable statutory provisions.

Since the National Criminal Code entered into force on 2 January 2026, Article 607 has constituted the principal statutory basis for the offence of money laundering. The provision preserves and consolidates the substance of Articles 3, 4, and 5 of Law No. 8 of 2010, which were repealed upon the Code's enactment. This continuity is confirmed by Law No. 1 of 2026 on Criminal Adjustments, which directs that references to the money-laundering provisions formerly contained in Articles 3, 4, and 5 of the 2010 Law be understood as references to Article 607 of the Criminal Code. Accordingly, the repeal of the former provisions did not create a substantive legal gap; rather, it transferred their operative content into the new codified framework. Article 607 therefore supplies the relevant legal basis for assessing the liability of mule-account holders who receive, control, transfer, or otherwise deal with proceeds derived from digital fraud.

Article 607 expressly treats fraud as a predicate offence, thereby bringing funds obtained through digital fraud within the scope of criminal proceeds capable of being laundered. This applies irrespective of whether the fraud is committed through conventional means or digital technologies; the decisive issue is whether the conduct satisfies the statutory elements of fraud and generates property derived from that offence. Accordingly, the use of online platforms, electronic payment systems, or intermediary accounts does not alter the legal character of the proceeds or prevent the subsequent application of Article 607.

The classification of fraud as a predicate offence is significant because it establishes the legal link between the underlying deception and the later handling of the funds. A mule-account holder's receipt, transfer, withdrawal, conversion, or use of funds may therefore constitute a separate money-laundering offence when accompanied by the requisite knowledge or reasonable suspicion. However, the mere fact that fraud proceeds pass through an account does not automatically establish liability: the prosecution must still connect the relevant transaction to criminal proceeds and prove the account holder's legally required mental state. The predicate offence need not necessarily be prosecuted through a separate, completed proceeding before money-laundering liability can be examined, but its essential factual and legal basis must nevertheless be established.

Although money laundering depends on the existence of criminal proceeds, Article 69 of Law No. 8 of 2010, which remains in force, establishes the procedural independence of money-laundering proceedings by providing that the predicate offence need not be finally proved before the investigation, prosecution, or trial of the laundering offence may commence. The provision prevents law enforcement from being required to await a final and binding judgment in the underlying fraud case. It does not, however, eliminate the prosecution's obligation to establish that the relevant property was derived from criminal conduct. Rather, the existence of the predicate offence may be determined incidentally within the money-laundering proceedings, on the basis of evidence sufficient to establish the criminal origin of the property and the accused's legally required mental state. Accordingly, Article 69 removes the requirement of a prior conviction, not the requirement to prove the factual and legal foundation of the predicate offence.

Active Money Laundering by a Mule Account Holder

Article 607 covers placing, transferring, assigning, spending, paying, granting, depositing, carrying abroad, transforming, exchanging, or otherwise dealing with property that the offender knows or reasonably suspects to constitute criminal proceeds. However, the performance of one of these acts does not, by itself, establish active money laundering. The conduct must also be undertaken for the purpose of concealing or disguising the property's criminal origin. Accordingly, liability depends on both the objective handling of illicit property and the prosecution's ability to demonstrate the legally required concealment purpose. This requirement distinguishes active money laundering from an innocent transaction involving funds later shown to be criminal proceeds and from passive receipt or control without evidence of an intention to obscure their origin.

A mule-account holder may satisfy this provision where the holder does more than passively receive funds and instead exercises control over them in a manner capable of disrupting their traceability. Relevant conduct may include distributing the funds among several accounts, withdrawing them in cash, converting them into crypto-assets, purchasing high-value goods, or transferring them to another account at the direction of the principal offender. These acts are legally significant because they can distance the proceeds from the fraud, obscure their movement, and facilitate their eventual use or dissipation. Nevertheless, such conduct does not establish active money laundering automatically. The prosecution must also demonstrate that the holder knew or reasonably suspected the criminal origin of the property and acted with the purpose of concealing or disguising that origin. Thus, the same transaction may constitute innocent assistance, passive receipt, or active money laundering depending on the holder's knowledge, degree of control, and purpose in handling the funds.

The feature distinguishing active money laundering from ordinary receipt is not the transfer of funds alone, but the purpose underlying that transfer. A transfer becomes legally significant under Article 607 only where the holder acts to conceal or disguise the funds' criminal origin, thereby obscuring their connection with the fraud that generated them. Accordingly, the prosecution must establish both that the holder dealt with property known or reasonably suspected to be criminal proceeds and that the dealing was undertaken for the requisite concealment or disguise purpose. The mere fact that funds were transferred, withdrawn, or delivered to another person is therefore insufficient without evidence that the holder's conduct was intended, or was objectively directed, to make the proceeds more difficult to trace or connect to the underlying fraud. That purpose may be inferred from the following circumstances:

- The funds are transferred immediately after receipt.
- Transfers are routed through several accounts.
- Transactions are divided into smaller amounts.
- Funds are withdrawn in cash and delivered to another person.
- The account holder uses false transaction descriptions.

- The account holder retains part of the money as commission.
- The holder deletes communications or gives false information about the source of the funds.

In the hypothetical case, A does more than merely make an account available: A actively transfers and withdraws the funds at B's direction. Those acts constitute direct dealings with the proceeds and may materially disrupt their traceability. If the prosecution proves that A knew or reasonably suspected that the funds derived from fraud and that A acted with the purpose of concealing or disguising their criminal origin, A's conduct may satisfy Article 607. The decisive issue is therefore not the transfer or withdrawal alone, but whether A's deliberate handling of the funds was objectively capable of obscuring their connection to the underlying fraud and was undertaken for that concealment purpose. Evidence that A transferred the funds immediately after receipt, withdrew them in cash, delivered them to B, retained a commission, or otherwise made the proceeds more difficult to trace would substantially strengthen the inference of active money laundering. Without proof of the requisite knowledge or reasonable suspicion and concealment purpose, however, the same conduct may amount only to passive receipt or control, or may be insufficient to establish criminal liability altogether.

Article 607 may also apply where A directly conceals or disguises the origin, source, location, intended use, transfer of title, or beneficial ownership of criminal proceeds. Such conduct may independently satisfy the active money-laundering provision where A acts with knowledge or reasonable suspicion that the property derives from an offence and with the purpose of making its criminal origin or ownership more difficult to identify. The relevant paragraph must, however, be applied in accordance with the specific acts proved and the formulation of the charge. The same conduct must not be characterised twice or used both to establish overlapping offences and to aggravate the same liability without a distinct legal and factual basis.

Passive Money Laundering by a Mule Account Holder

Article 607 imposes liability on any person who receives, controls, places, transfers, pays, gives, donates, deposits, exchanges, or uses property that the person knows or reasonably suspects constitutes criminal proceeds. This provision is commonly understood as passive money laundering because liability may arise from the person's receipt, control, or use of illicit property even without proof that the person personally committed the predicate offence or actively concealed the property's origin. The provision therefore targets the subsequent handling of criminal proceeds rather than the person's role in generating them. Its central inquiry is whether the person accepted or exercised control over property in circumstances that established knowledge or provided sufficient grounds to suspect its criminal origin. Accordingly, a mule-account holder may incur liability merely by receiving or controlling fraud proceeds where the surrounding circumstances demonstrate that the holder knew or reasonably suspected their unlawful source, even if the holder did not personally deceive the victim or undertake additional steps to disguise the funds. This form of liability reflects the broad scope of money laundering statutes, which often encompass the mere possession, acquisition, or use of property tainted by criminal activity (Aebi et al., 2010; Chaudhary & Kale, 2024).

Unlike the active money-laundering provision in Article 607, this paragraph does not require proof that the accused acted with the specific purpose of concealing or disguising the origin of the property. Its focus is instead on the knowing or suspicious receipt, control, or use of property derived from an offence. Accordingly, liability may arise even where the account holder did not take steps to obscure the funds' origin, provided that the prosecution proves that the holder knew or reasonably suspected their criminal source. The absence of a concealment purpose therefore does not preclude liability; it distinguishes passive money laundering from the more deliberate concealment-based conduct covered by the active provision. This objective threshold aligns with international standards, which establish that criminal liability for passive laundering attaches when an individual accepts or retains assets while harboring reasonable suspicions of their illicit provenance (Bahari et al., 2025).

This provision is highly relevant to an account holder who did not participate directly in deceiving the victim but knowingly received or controlled the proceeds. A need not know the victim's identity, communicate with the victim, or personally create the fraudulent link to incur liability. The critical issue is whether A knew or reasonably suspected that the funds were criminal proceeds when A received or exercised control over them. Thus, where an unusually large or unexplained amount enters A's account and A nevertheless transfers the funds to B in exchange for a commission, those circumstances may demonstrate both control over criminal property and culpable awareness of its unlawful source. The commission is particularly significant because it provides evidence that A did not act as a merely passive intermediary but deliberately participated in handling the proceeds despite circumstances that should have prompted suspicion. Such regulatory requirements create a framework where professionals and account holders are subject to heightened vigilance, as a failure to satisfy due diligence can be interpreted as wilful or negligent omission (Benson & Bociga, 2024).

The judicial decision annotation published by PPATK indicates that knowledge or reasonable suspicion should be assessed from the totality of the circumstances, rather than inferred solely from the account holder's formal ownership of the account. Relevant factors include the profile and occupation of the person requesting or borrowing the account, the economic reasonableness of the compensation offered, the account holder's relationship with that person, and the holder's response to circumstances that would make the transaction suspicious. On this approach, receiving and controlling funds through another person's account may constitute passive money laundering where the surrounding facts gave the holder sufficient grounds to suspect that the funds were derived from an offence. The significance of these factors lies in their cumulative force: an unusual transaction, inadequate explanation, and economically irrational compensation may collectively establish culpable suspicion even if no single circumstance conclusively proves knowledge. Accordingly, a holder cannot avoid liability merely by claiming ignorance where the holder deliberately accepted control of the account, benefited from the arrangement, and disregarded obvious indicators of its unlawful purpose. In the Indonesian legal context, this framework aligns with Article 5 of Law Number 8 of 2010, which penalizes individuals who receive or control assets they know or reasonably suspect are derived from criminal acts (Wardani et al., 2022).

If A gives B unrestricted access to the account, despite knowing that B has no clear occupation or legitimate economic explanation, and receives compensation lacking a reasonable economic basis, those circumstances may establish that A had sufficient grounds to suspect that the account would be used unlawfully. The inference is substantially strengthened if A knows that a large and unexplained sum has entered the account, nevertheless permits or facilitates withdrawals, and retains a share of the funds. Viewed cumulatively, these facts indicate more than mere negligence or passive involvement: they may demonstrate that A knowingly accepted control over potentially criminal proceeds while disregarding obvious indicators of their unlawful origin. Although no single circumstance is necessarily conclusive, their combined effect may satisfy the requirement of knowledge or reasonable suspicion under Article 607.

Conversely, criminal liability should not be imposed where the account is used through hacking, identity theft, or unauthorised access takeover without the holder's knowledge, intention, or effective control. In such circumstances, the holder lacks the requisite connection to both the predicate offence and the subsequent handling of the proceeds. A prompt report to the bank or law-enforcement authorities, the absence of personal benefit or compensation, no relationship or communication with the offender, and the lack of control over the relevant transaction instruments may collectively demonstrate that the holder neither knew nor had reasonable grounds to suspect the criminal source of the funds. These circumstances are particularly significant where the holder takes reasonable steps to secure the account, assists in tracing or recovering the funds, and does not voluntarily permit withdrawals or transfers. Mere formal ownership of the account, without proof of knowing participation, control, or culpable disregard of suspicious circumstances, should therefore be insufficient to establish liability under either the predicate

offence or the money-laundering provision.

Relationship Between Participation in Fraud and Money Laundering

A mule-account holder may participate in the predicate offence and also incur separate liability for money laundering. These forms of liability are not necessarily mutually exclusive because they address different criminal conduct: participation liability concerns the holder's contribution to bringing about the fraud, whereas money-laundering liability concerns the subsequent receipt, control, use, or transfer of the fraudulently obtained proceeds (Halliday et al., 2024; Sarumaha et al., 2023). Accordingly, the same conduct may support both forms of liability where the evidence establishes, first, that the holder intentionally assisted the fraudulent scheme and, second, that the holder knowingly or reasonably suspected the criminal origin of the funds and dealt with them in a manner prohibited by law. The two liabilities must, however, remain analytically distinct and be supported by facts satisfying the elements of each offence. While the predicate fraud often generates the illicit capital, the subsequent layering process, where funds are moved through various accounts to obscure their origins, frequently relies on the active facilitation provided by these mules (Rani et al., 2023).

If A provides the account pursuant to the fraudulent plan and, once the funds arrive, transfers or otherwise handles them to conceal their criminal origin, A's conduct may support two analytically distinct forms of liability. First, surrendering the account and cooperating with the principal before or during the fraud may constitute joint commission or intentional assistance in the predicate offence, depending on A's knowledge, role, and contribution to the scheme. Second, receiving, controlling, withdrawing, or transferring the proceeds after the fraud may independently satisfy the elements of money laundering, provided that A knew or reasonably suspected their criminal origin and dealt with them in a manner prohibited by law. The two forms of liability are therefore not interchangeable: participation concerns A's contribution to producing the illicit proceeds, whereas money laundering concerns A's subsequent dealings with those proceeds. Their concurrent application is justified only where the evidence establishes both the requisite involvement in the fraudulent plan and a separate, culpable act of receiving, controlling, or concealing the resulting funds. Integrating these investigative efforts into a unified framework, often termed "FRAML," allows financial institutions to harmonize fraud prevention and anti-money laundering protocols, ensuring that the interplay between predicate crimes and subsequent asset concealment is addressed comprehensively (Sullivan, 2023).

The simultaneous application of both legal constructions must rest on clearly established and analytically distinct facts. Law-enforcement authorities may not infer participation in fraud solely from the receipt of its proceeds, because post-offence possession or handling does not, without more, prove that the person contributed to the fraudulent scheme itself. Conversely, participation in the predicate offence does not automatically establish money-laundering liability. The prosecution must separately prove that, after or in connection with the fraud, the person received, controlled, used, withdrew, transferred, or otherwise dealt with criminal proceeds in a manner falling within Article 607. Accordingly, the same evidence must not be counted twice to establish both offences without identifying the distinct conduct and mental element supporting each form of liability. Where those separate requirements are not proved, the person may be liable for only the offence established by the evidence, rather than being subjected to cumulative liability based merely on the account's involvement in the transaction.

CONCLUSION

The criminal liability of a mule-account holder cannot be determined by formal ownership of the account through which a victim's funds passed, but depends on the timing and form of involvement, the degree of cooperation, control over the account, and the holder's knowledge and intention. A holder who knew of the fraudulent plan from the outset, cooperated closely with the principal offender, and knowingly performed part of that plan is liable as a joint perpetrator; a holder who was not closely involved in

executing the fraud but intentionally provided an account or banking access to facilitate it is properly classified as an accessory; and a holder whose account or identity was used without knowledge or intention cannot be liable for the predicate offence. Separately, a holder incurs money-laundering liability where the holder receives, controls, uses, withdraws, or transfers funds known or reasonably suspected to derive from digital fraud, passive laundering arising from knowing receipt or control, and active laundering where funds are transferred, divided, withdrawn, transformed, or assigned for the purpose of concealing their origin. Because knowledge or reasonable suspicion must be established objectively from the totality of the circumstances, such as surrendering all banking access, accepting unreasonable compensation, transactions inconsistent with the holder's economic profile, rapid movement of funds, or layered transaction patterns, no single circumstance should determine guilt. The two forms of liability may therefore coexist, but only where they rest on clearly distinguishable acts, since participation concerns the holder's contribution to producing the illicit proceeds while money laundering concerns their subsequent receipt, control, use, or concealment. Enforcement should accordingly prioritise the holder's factual role and mental state over the name recorded in banking records, allowing knowing facilitators to be held proportionately liable while protecting account holders who are genuine victims of hacking, identity theft, or unauthorised access.

REFERENCES

- Aebi, M. F., Harrendorf, S., & Jehle, J.-M. (2010). *Defining and registering criminal offences and measures*. Göttinger Studien zu den Kriminalwissenschaften. <https://doi.org/10.17875/gup2010-188>
- Alhajeri, R., & Alhashem, A. (2023). Using artificial intelligence to combat money laundering. *Intelligent Information Management*, 15(4), 284–305. <https://doi.org/10.4236/iim.2023.154014>
- Anastasia, P., Asher, F., & Nicola, H. (2019). *The human factor of cybercrime*. <https://doi.org/10.4324/9780429460593>
- Bahari, B. S., Priyatno, D., Handayani, T., & Rusman, R. (2025). Criminal liability of passive money laundering perpetrators. *Intellectual Law Review (ILRE)*, 3(1), 49–59. <https://doi.org/10.59108/ilre.v3i1.75>
- Baker, D. J. (2016). Lesser included offences, alternative offences and accessorial liability. *The Journal of Criminal Law*, 80(6), 446–464. <https://doi.org/10.1177/0022018316675817>
- Bekkers, L., van Houten, Y., Spithoven, R., & Leukfeldt, R. (2023). Money mules and cybercrime involvement mechanisms: Exploring the experiences and perceptions of young people in the Netherlands. *Deviant Behavior*, 44(9), 1368–1385. <https://doi.org/10.1080/01639625.2023.2196365>
- Benson, K., & Bociga, D. (2024). Occupation, organisation, opportunity, and oversight: Law firm client accounts and (anti-)money laundering. *European Journal on Criminal Policy and Research*, 30(3), 449–473. <https://doi.org/10.1007/s10610-024-09581-1>
- Berry, M., Salinas, M., & Gundur, R. V. (2023). Financial risk management strategies of small to medium illicit drug enterprises: Considering low-level money laundering. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-023-09501-5>
- du Bois-Pedain, A. (2019). Participation in crime. In *Cambridge University Press eBooks* (pp. 94–134). Cambridge University Press. <https://doi.org/10.1017/9781108649742.004>
- Bulut, İ. (2024). Banka hesaplarının kullanılması ve ceza sorumluluğu. *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 14(2), 719–756. <https://doi.org/10.54704/akdhfd.1556442>
- Chaudhary, S., & Kale, S. P. (2024). Vijay Madanlal Choudhary v Union of India: A systematic breakdown of protections against testimonial compulsion during criminal investigations. *Jindal Global Law Review*, 15(1), 89–117. <https://doi.org/10.1007/s41020-024-00220-8>
- Chen, X. H., You, X., & Chang, V. (2021). FinTech and commercial banks' performance in China: A leap forward or survival of the fittest? *Technological Forecasting and Social Change*, 166, 120645. <https://doi.org/10.1016/j.techfore.2021.120645>

- Custers, B., Pool, R., & Cornelisse, R. (2018). Banking malware and the laundering of its profits. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3411486>
- Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y. C., & Mejía, D. D. (2021). Evaluating criminal transactional methods in cyberspace as understood in an international context. *CrimRxiv*. <https://doi.org/10.21428/cb6ab371.5f335e6f>
- Halliday, T. C., Levi, M., & Reuter, P. H. (2024). Anti-money laundering: An inquiry into a disciplinary transnational legal order. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4897094>
- Huang, H. (2024). Criminalization challenge and analysis of network crime assistance behaviors. *Journal of Politics and Law*, 17(2), 59. <https://doi.org/10.5539/jpl.v17n2p59>
- Hülse, R. (2017). The money mule. *Vanderbilt Journal of Transnational Law*. <https://epub.ub.uni-muenchen.de/57714/>
- Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber security and digital economy: Opportunities, growth and challenges. *Journal of Technology Innovations and Energy*, 3(2), 1–22. <https://doi.org/10.56556/jtie.v3i2.907>
- Kupczyński, J. (2025). Strawman—An indispensable element in many cybercrimes: A legal and forensic perspective on the role of a strawman in crimes committed remotely. *Cybersecurity & Cybercrime*, 1(7), 75–91. <https://doi.org/10.5604/01.3001.0055.1582>
- Leukfeldt, R., Lavorgna, A., & Kleemans, E. R. (2016). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287–300. <https://doi.org/10.1007/s10610-016-9332-z>
- Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice*, 49, 579–631. <https://doi.org/10.1086/708047>
- Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and risks of blockchain technologies: A research agenda. *Proceedings of the 50th Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/HICSS.2017.185>
- Martin, G. (2025). Cybercrime. In *The Blackwell encyclopedia of sociology* (pp. 1–3). <https://doi.org/10.1002/9781405165518.wbeosc194.pub2>
- Muk, Y. H. T. (2025). From “knowing destruction” to “magnificent crime”: Re-evaluating the standards for knowingly in the crime of assisting information network criminal activities. *Lecture Notes in Education Psychology and Public Media*, 119(1), 239–247. <https://doi.org/10.54254/2753-7048/2025.lid30581>
- Pane, L. T., Sunarmi, S., Mulyadi, M., & Andriati, S. L. (2024). Optimalisasi penegakan hukum pidana terhadap tindak pidana pencucian uang dengan modus jual beli rekening bank. *Jurnal Ilmu Hukum Humaniora dan Politik*, 4(5), 1333–1344. <https://doi.org/10.38035/jihhp.v4i5.2208>
- Patsakis, C., Politou, E., Alepis, E., & Hernández-Castro, J. (2023). Cashing out crypto: State of practice in ransom payments. *International Journal of Information Security*, 23(2), 699–712. <https://doi.org/10.1007/s10207-023-00766-z>
- Rani, M. I. A., Nazri, S. N. F. S. M., & Zolkafil, S. (2023). A systematic literature review of money mule: Its roles, recruitment and awareness. *Journal of Financial Crime*, 31(2), 347–361. <https://doi.org/10.1108/JFC-10-2022-0243>
- Sarkar, G., Putrevu, V. S. C., & Shukla, S. K. (2026). Understanding Jamtara cybercriminals: Poverty, opportunity, and the rise of organized criminal networks. *Humanities and Social Sciences Communications*. <https://doi.org/10.1057/s41599-026-07703-0>
- Sarumaha, F., Gaol, S. L., & Sujono. (2023). Comparative study of criminal liability of offenders committing fraud and money laundering together as continuing actions. *International Journal of Science and Society*, 5(1), 433–448. <https://doi.org/10.54783/ijssoc.v5i1.729>
- Schmitt, M., & Fléchais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(12). <https://doi.org/10.1007/s10462-024-10973-2>
- Sudirman, L., & Disemadi, H. S. (2022). Legal protection for borrowers and business dispute resolution in fintech lending services. *Jurnal Jurisprudence*, 11(2), 187–204. <https://doi.org/10.23917/>

[jurisprudence.v11i2.15853](#)

- Sullivan, K. (2023). Fraud and anti-money laundering. In *Apress eBooks* (pp. 219–229). https://doi.org/10.1007/979-8-8688-0066-5_9
- Tambunan, H., & Barthos, M. (2025). Criminal liability of individuals and third parties in crypto-asset-based fraud schemes: A dormant responsibility perspective. *Greenation International Journal of Law and Social Sciences*, 3(3), 1084–1093. <https://doi.org/10.38035/gijlss.v3i3.596>
- Wardani, A., Ali, M., & Barkhuizen, J. (2022). Money laundering through cryptocurrency and its arrangements in Money Laundering Act. *Lex Publica*, 9(2), 49–66. <https://doi.org/10.58829/lp.9.2.2022.49-66>
- Wells, C., & Quick, O. (2012). Offence preparation and participation. In *Cambridge University Press eBooks* (pp. 292–336). Cambridge University Press. <https://doi.org/10.1017/CBO9780511751028.012>
- Zali, M., & Maulidi, A. (2018). Fighting against money laundering. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3296154>
- Zezyulina, T. A. (2026). A new approach to criminalizing droppers: Problems and prospects. *Journal of Law and Administration*, 21(4), 56–64. <https://doi.org/10.24833/2073-8420-2025-4-77-56-64>
- Zhan, Y. (2025). Correcting judicial misconceptions regarding the “knowing” element in payment settlement-related cybercrime cases involving helping information network crime. *Lecture Notes in Education Psychology and Public Media*, 128(1), 135–141. <https://doi.org/10.54254/2753-7048/2025.Id28549>