INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FROM UNWITTING ACCOUNT HOLDER TO KNOWING FACILITATOR: DETERMINING CRIMINAL LIABILITY IN MONEY MULE CASES

AUTHORED BY - THOWFIK AHAMED
LLM-Criminal Law – Second Year, Crescent School of Law,
B. S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai, Tamilnadu

ABSTRACT

The increasing use of bank accounts and digital payment instruments to receive, transfer and withdraw proceeds of cyber-enabled financial crime has created a difficult question of criminal responsibility: when does a money mule become a criminal participant rather than an unwitting intermediary? The issue has acquired particular significance in Tamil Nadu following the Cyber Crime Wing's 48-hour statewide special drive against mule account holders, during which 837 persons were reportedly arrested in connection with 601 cases involving 9,804 complaints and fraudulent transactions exceeding ₹545 crore. This enforcement action highlights both the growing role of mule accounts in cybercrime and the need to determine the individual culpability of persons whose accounts are used in such transactions. This article adopts a doctrinal approach to examine the criminal liability of money mules under Indian law, with particular emphasis on mens rea, knowledge, intention, "reason to believe," abetment, conspiracy and money laundering. It proposes a five-fold analytical classification of account holders as unauthorised or innocent, unwitting, negligent, reckless or deliberately blind, and knowing and intentional participants. The article argues that the mere appearance of an account in a financial trail, receipt of criminal proceeds, or receipt of a nominal commission should not, by itself, establish criminal liability. Instead, liability must depend upon the conduct proved, the degree of culpability established and the specific mental element required by the offence charged. The article further examines the evidentiary challenges involved in inferring knowledge from transaction patterns, financial benefits, communications and surrounding circumstances. It proposes a Culpability–Mens Rea Framework to distinguish genuinely unwitting account holders from intentional facilitators while preserving effective enforcement against cybercrime networks.

ISSN: 2582-6433

Keywords: Money Mules; Mens Rea; Cybercrime; Money Laundering; Abetment; Reason to Believe;A Criminal Liability.

1. INTRODUCTION

The rapid expansion of digital banking, online payment systems and internet-enabled financial transactions has created new opportunities for cybercriminals to move and conceal the proceeds of fraud. One important mechanism through which such proceeds are transferred is the use of money-mule accounts. A money mule may provide a bank account or other financial facility through which illicit funds are received, transferred or withdrawn, thereby functioning as an intermediary within a wider cybercrime network. However, the mere use of a person's account in the movement of criminal proceeds does not necessarily establish that the account holder possessed the knowledge or intention required for criminal liability.

The issue has acquired immediate significance in Tamil Nadu. On 6 August 2026, the Cyber Crime Wing of the Tamil Nadu Police commenced a 48-hour statewide special drive against mule account holders. According to The Hindu, 837 persons were arrested in connection with 601 cases involving 9,804 complaints and fraudulent transactions exceeding ₹545 crore. The operation targeted persons involved in opening, operating and facilitating the misuse of bank accounts for receiving and withdrawing proceeds of cyber fraud. The police also relied upon cybercrime complaint databases and financial fund-trail analysis to identify persons connected with the transactions.

The scale of this enforcement action demonstrates the importance of disrupting the financial infrastructure of cybercrime. At the same time, it raises a significant question of individual criminal responsibility. Persons whose accounts are connected with cybercrime may occupy substantially different positions. An account may be used without the holder's knowledge; an individual may voluntarily provide an account without knowing its criminal purpose; another may ignore suspicious circumstances; while a further individual may knowingly and intentionally facilitate the movement of illicit funds. Treating these circumstances as legally identical may undermine the principle that criminal liability depends upon the conduct and mental state required by the particular offence.

The central research problem of this article is therefore whether Indian criminal law adequately distinguishes between unwitting money mules and knowing or intentional facilitators of cybercrime. The article adopts a doctrinal methodology and examines the relevant principles under the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000 and the Prevention of Money-Laundering Act, 2002, with particular emphasis on mens rea, knowledge,

ISSN: 2582-6433

intention, "reason to believe," abetment and criminal participation.

The article argues that being a conduit for criminal proceeds should not, by itself, determine criminal liability. Instead, liability should be assessed by examining the person's degree of culpability, the conduct proved against them and the specific mental element required by the offence charged. On this basis, the article proposes a Culpability–Mens Rea Framework to distinguish genuinely unwitting account holders from persons who knowingly or deliberately facilitate cybercrime, while maintaining effective criminal enforcement against money-mule networks.

2. CONCEPTUALISING MONEY MULES AND DEGREES OF CULPABILITY

A "money mule" is generally understood as a person whose bank account or other financial facility is used to receive, transfer or withdraw funds connected with criminal activity[1]. In cyber-enabled financial crime, such persons may function as intermediaries between the perpetrators of the underlying fraud and the eventual movement of illicit funds[2]. Their involvement can make the tracing of criminal proceeds more difficult and may assist wider cybercrime networks in distancing themselves from the financial consequences of their conduct[3]. However, the expression "money mule" describes a functional role in the movement of funds and should not, by itself, be treated as a conclusion of criminal liability.

The circumstances in which individuals become involved in mule-account arrangements can differ significantly. Some accounts may be used without the holder's knowledge or consent. Others may be voluntarily provided in exchange for a small payment without the individual understanding that the account will be used for criminal purposes[4]. Some account holders may subsequently encounter circumstances suggesting that the transactions are unlawful but continue to participate, while others may knowingly and deliberately facilitate the movement of criminal proceeds. These differences are significant because criminal responsibility depends

[1] *Professional Money Laundering* 22 (2018), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf [https://perma.cc/xxxx-xxxx]; Reserve Bank of India, Circular No. RPCD.CO.RRB.AML.BC.No.40/03.05.33(E)/2010-11, *Operation of Bank Accounts & Money Mules* (Dec. 24, 2010).

[2] Interpol & Egmont Grp., *Illicit Financial Flows from Cyber-Enabled Fraud* 3 (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf [https://perma.cc/xxxx-xxxx].

[3] *Id.*; *see also RBI Asks Banks to Collaborate with MuleHunter.AI to Find Mule Accounts*, Bus. Standard (Dec. 6, 2024), https://www.business-standard.com/finance/news/rbi-asks-banks-to-collaborate-with-mulehunter-ai-to-find-mule-accounts-124120600623_1.html.

[4] *Professional Money Laundering*, *supra* note 1, at 22.

ISSN: 2582-6433

not merely upon the physical connection between an individual and a transaction but also upon the mental element required by the particular offence[5].

Proposed Classification of Money Mules

For the purposes of this article, money mules are classified according to their degree of knowledge and participation. This classification is proposed as an analytical framework for the present study and is not a statutory classification recognised by Indian legislation or judicial precedent[6].

Category	Knowledge	Nature of participation	Degree of culpability
1. Unauthorised / Innocent Account Holder	No knowledge	Account used without knowledge or consent	None or minimal
2. Unwitting Money Mule	No knowledge of criminal purpose	Voluntarily provides account for an apparently legitimate purpose or small payment	Low/absent mens rea
3. Negligent Money Mule	No actual knowledge, but suspicious circumstances may exist	Fails to exercise reasonable caution or make appropriate inquiries	Dependent upon the offence and statutory mental element
4. Reckless / Deliberately Blind Money Mule	Significant suspicion or conscious avoidance of knowledge	Continues facilitating transactions despite serious warning signs	Intermediate/high culpability
5. Knowing / Intentional Money Mule	Actual knowledge of criminal purpose	Deliberately receives, transfers, withdraws or facilitates criminal proceeds	High culpability

[5] *See* Srinivas Mall Bairoliya v. Emperor, AIR 1947 PC 135; State of Maharashtra v. Mayer Hans George, AIR 1965 SC 722; Bharatiya Nyaya Sanhita, 2023, § 2(24) (India). *See generally* K.D. Gaur, *Textbook on the Indian Penal Code* (6th ed. 2016) (discussing the maxim *actus non facit reum nisi mens sit rea* as the foundation of mens rea in Indian criminal law).

[6] *Professional Money Laundering* 22 (2018); the categories proposed here are the author's own formulation for the purposes of Indian criminal law analysis.

ISSN: 2582-6433

The classification highlights a spectrum extending from absence of knowledge to deliberate participation[7]. It is particularly important to distinguish the unwitting money mule from the knowing or deliberately facilitating participant. A person may voluntarily provide an account and even receive a small payment without understanding that the account will be used for cyber fraud. Conversely, a person who knowingly assists the movement of criminal proceeds may occupy a substantially different legal position[8].

The classification also highlights the distinction between financial connection and criminal participation. The fact that criminal proceeds have passed through a person's account may establish a factual connection with the transaction, but it does not necessarily establish knowledge, intention or participation sufficient for every offence[9]. The central inquiry is therefore not simply whether an account was used, but what the account holder knew, what the account holder intended, what the account holder did, and whether those facts satisfy the legal requirements of the offence charged.

This distinction is particularly important in cases involving persons who provide their accounts for a small financial benefit without awareness of the underlying cybercrime[10]. At the same time, the classification does not suggest that every claim of ignorance should be accepted automatically. The person's conduct, surrounding circumstances and available evidence must be examined to determine whether the required mental element can be established.

Thus, the proposed classification provides the conceptual foundation for examining the Indian legal framework and, more importantly, for determining when an individual's involvement in the movement of criminal proceeds crosses the threshold from an innocent or unwitting financial connection to legally sufficient criminal participation.

[7] *See* Prevention of Money Laundering Act, No. 15 of 2003, § 3 (India) (imposing liability on a person who "knowingly assists or knowingly is a party or is actually involved" in dealing with proceeds of crime); Bharatiya Nyaya Sanhita, 2023, § 2(24) (India).

[8] Vijay Madanlal Choudhary v. Union of India, (2022) SCC OnLine SC 929 (holding that knowledge that property constitutes proceeds of crime is not a condition precedent for prosecution under § 3 of the PMLA where the statutory language of "indirect" involvement is satisfied), *with* Pavana Dibbur v. Directorate of Enforcement, (2023) SCC OnLine SC 1586 (clarifying that mere participation in a transaction connected to a scheduled offence does not, without more, establish the offence of money laundering, and that the prosecution must connect the specific accused to conduct falling within § 3).

[9] Pavana Dibbur v. Directorate of Enforcement, (2023) SCC OnLine SC 1586; *see also* S. Srinivasan v. Assistant Director, Directorate of Enforcement, [Madras High Court decision on possession of proceeds of crime and the limits of Section 3 PMLA] (noting the risk that a purely literal reading of "possession" could expose persons without genuine knowledge to prosecution).

[10] *Professional Money Laundering*, *supra* note 1, at 22.

ISSN: 2582-6433

3. INDIAN LEGAL FRAMEWORK AND MENS REA

The criminal liability of a money mule in India must be determined by reference to the specific offence alleged rather than by treating "money mule" as an independent offence. Depending upon the facts, the conduct of an account holder may potentially attract provisions relating to cheating, dishonest receipt or retention of property, abetment, criminal conspiracy, cyber offences or money laundering[11]. The applicable legal framework is therefore dispersed across the **Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology Act, 2000 and the Prevention of Money-Laundering Act, 2002 (PMLA).**

The BNS is particularly relevant where the account holder is alleged to have assisted the commission of a fraud or knowingly dealt with property connected with an offence[12]. In such cases, the distinction between the physical act of receiving or transferring funds and the mental element accompanying that conduct becomes important. A person who knowingly assists a fraudulent scheme occupies a different legal position from a person who provides an account without knowing its criminal purpose[13]. Similarly, the provisions concerning abetment and criminal conspiracy require examination of the nature of the person's participation rather than merely their association with an account through which criminal proceeds passed[14].

The Information Technology Act, 2000 may become relevant where the money-mule arrangement forms part of a cyber-enabled offence involving electronic records, identity-related misuse, unauthorised access or other conduct falling within the Act[15]. However, the fact that a transaction occurred through an electronic banking or payment system does not, by itself, establish liability under the Information Technology Act. The specific statutory ingredients of the provision invoked must be established.

The PMLA introduces a further dimension where the funds handled through the mule account constitute proceeds of crime and the conduct falls within the statutory requirements of money laundering. Here, it is necessary to distinguish between the underlying cyber offence, the

[11] Bharatiya Nyaya Sanhita, 2023, Sec 61, 316–318, 317 (India); Information Technology Act, No. 21 of 2000, Sec 43, 66, 66C, 66D (India); Prevention of Money-Laundering Act, No. 15 of 2003, § 3 (India).

[12] BNS, 2023, § 318(4) (India) (corresponding to § 420 of the repealed Indian Penal Code, 1860, punishing cheating that dishonestly induces delivery of property); *id.* § 317 (corresponding to § 411 IPC, punishing dishonest receipt or retention of stolen property, an offence requiring "reason to believe" the property to be stolen)

[13] *See* Vijay Madanlal Choudhary v. Union of India, (2022) SCC OnLine SC 929; Pavana Dibbur v. Directorate of Enforcement, (2023) SCC OnLine SC 1586.

[14] BNS, 2023, § 61 (India) (corresponding to §§ 120A–120B of the repealed IPC, defining and punishing criminal conspiracy); *id.* § 45 (corresponding to § 107 IPC, on abetment by conspiracy). *See generally* Bhatt & Joshi Assocs., *Section 120B IPC / Section 61 BNS: Criminal Conspiracy vs. Abetment* (2026) (distinguishing abetment, which requires instigation, aiding or engagement in conspiracy toward a completed offence, from criminal conspiracy, which is complete upon agreement for a serious offence).

[15] Information Technology Act, 2000, §§ 43, 66, 66C (identity theft), 66D (cheating by personation using a computer resource)

ISSN: 2582-6433

generation of proceeds of crime and the subsequent conduct concerning those proceeds. A person who knowingly participates in dealing with proceeds of crime may therefore occupy a substantially different position from an account holder who receives funds without knowledge of their criminal origin[16].

Across these legal frameworks, mens rea becomes central to the distinction between innocent involvement and criminal participation. Knowledge, intention and "reason to believe" are not necessarily interchangeable concepts. Likewise, negligence or failure to make an inquiry should not automatically be treated as equivalent to actual knowledge unless the particular offence legally permits such an inference or standard.

This distinction is particularly important for the proposed classification of money mules. An unwitting account holder may have physically facilitated the movement of funds without possessing the mental element required by the offence. A negligent account holder may have acted carelessly, but carelessness alone does not necessarily establish criminal liability. A reckless or deliberately blind participant presents a more difficult case because suspicious circumstances may potentially support an inference concerning the person's state of mind[17]. At the other end of the spectrum, evidence of actual knowledge combined with deliberate assistance provides a substantially stronger basis for criminal responsibility.

Accordingly, the legal inquiry should proceed in two stages: first, identify the conduct attributable to the account holder; and secondly, determine whether the mental element required by the particular offence is established by the evidence. This approach prevents the label "money mule" from replacing the statutory analysis required for criminal conviction and provides the foundation for examining how courts may determine knowledge and participation from circumstantial evidence.

4. DETERMINING CRIMINAL LIABILITY: EVIDENCE AND JUDICIAL APPROACH

The principal difficulty in money-mule prosecutions is often not establishing that money passed through a particular account, but determining what the account holder knew about the transaction. Bank statements, transaction records and digital fund trails can establish the movement of money, but they do not necessarily reveal the mental state of the person operating

[16] Vijay Madanlal Choudhary, *supra* note 3, *with* Pavana Dibbur, *supra* note 3.
[17] *Professional Money Laundering* 22 (2018) (describing the spectrum from witting to unwitting mule participation).

ISSN: 2582-6433

the account[18]. Consequently, the determination of criminal liability requires a distinction between evidence establishing the financial transaction and evidence capable of establishing the knowledge or intention of the account holder.

In practice, the mental state of a money mule may have to be inferred from surrounding circumstances. Relevant circumstances may include the frequency and value of transactions, the identity of persons sending or receiving the money, the immediate withdrawal or transfer of funds, commissions or other financial benefits received, communications with recruiters, instructions regarding the handling of funds, attempts to conceal transactions and the conduct of the account holder after becoming aware of suspicious activity[19]. The significance of these circumstances must, however, be assessed cumulatively rather than by treating any single factor as conclusive proof of criminal knowledge.

The distinction between suspicion and legally sufficient knowledge is particularly important[20]. An individual may become suspicious because an unexpected amount enters the account, yet suspicion alone does not necessarily establish that the person knew the money represented proceeds of cybercrime. Similarly, receiving a small commission for allowing an account to be used may indicate participation in a financial arrangement, but it does not automatically establish knowledge of its criminal purpose[21]. The prosecution must therefore establish the mental element required by the particular offence through admissible evidence and permissible inference.

The concept of "reason to believe" presents a further doctrinal difficulty. Where a statute expressly employs this standard, the court must examine the circumstances known to the accused and determine whether they satisfy the statutory threshold[22]. It should not automatically be assumed that "reason to believe" is identical to actual knowledge, nor that mere negligence is sufficient[23]. The distinction becomes particularly important where an accused claims that they did not know the criminal origin of the funds but continued participating despite unusual circumstances.

---

[18] *See* Shiv Kumar v. State of Madhya Pradesh, (2022) 9 SCC 676; S.D. Shabuddin v. State of Telangana, 2025 INSC 999.

[19] *Professional Money Laundering* 22 (2018) (identifying frequency of transactions, immediate withdrawal, and recruiter communication as indicators considered in mule typologies).

[20] Shiv Kumar v. State of Madhya Pradesh, (2022) 9 SCC 676 (holding that it is "not enough to prove that the accused was either negligent or that he had a cause to think" that property was tainted; the "believe" element requires more than suspicion).

[21] *Id.*; *see also* Nanak Chand v. State of Punjab (illustrating that awareness inferred from surrounding circumstances, such as inexplicably low prices or neighbourhood proximity to the offence, may satisfy "reason to believe" where mere possession would not)

[22] Trimbak v. State of M.P., AIR 1954 SC 39; Mohan Lal v. State of Maharashtra, (1979) 4 SCC 751; Shiv Kumar v. State of Madhya Pradesh, (2022) 9 SCC 676.

[23] Shiv Kumar v. State of Madhya Pradesh, (2022) 9 SCC 676.

ISSN: 2582-6433

The person's conduct before and after the transaction may also be relevant. Communications with recruiters, repeated transactions, deletion of messages, attempts to conceal financial activity or continued participation after warnings may potentially strengthen an inference of knowledge. Conversely, promptly informing the bank, discontinuing the arrangement or cooperating with an investigation may be relevant to the assessment of the person's explanation. Such circumstances should not be treated mechanically; their evidentiary value depends upon the facts of the individual case.

The Tamil Nadu enforcement operation illustrates why this evidentiary distinction is practically significant. The police reportedly relied upon the National Cybercrime Reporting Portal, the Pratibimb portal and financial fund-trail analysis to identify persons associated with mule accounts[24]. Such investigative tools can establish links between accounts and cybercrime complaints, but the subsequent judicial inquiry remains distinct: whether the individual account holder possessed the mental element necessary for the offence alleged.

The central evidentiary principle, therefore, should be that financial tracing cannot substitute for proof of criminal culpability. A transaction trail may show where money travelled; it does not, without more, establish why the account holder participated or what the person knew. This is particularly significant for unwitting and low-level money mules who may have been recruited through apparently legitimate employment or financial opportunities.

Accordingly, judicial assessment should move beyond the question of "Whose account received the money?" and examine "What did the account holder know, what did the account holder do, and what does the totality of circumstances establish about the person's culpability?" This approach allows courts to distinguish an unwitting intermediary from a person who deliberately facilitates cybercrime and provides the basis for identifying the doctrinal gap addressed in the following section.

5. THE DOCTRINAL GAP AND THE PROPOSED CULPABILITY–MENS REA FRAMEWORK

The existing legal framework provides several mechanisms through which persons involved in the movement of criminal proceeds may be prosecuted. However, a significant doctrinal

[24] 'Tamil Nadu Cops Go on "Mule Hunt", Arrest 837 Account Holders in Two-Day Statewide Drive', DT Next (Chennai, Aug. 2026), https://www.dtnext.in/news/tamilnadu/837-mule-account-holders-facilitating-cyber-cons-arrested-in-tamil-nadu (reporting the operation covered 9,804 NCRP complaints involving fraudulent transactions of ₹545.27 crore); Press Trust of India, *'Samanvaya' Portal for Data Exchange Among Police Forces on Cyber Criminals' Activities*, Deccan Herald, https://www.deccanherald.com/india/samanvaya-portal-for-data-exchange-among-police-forces-on-cyber-criminals-activities-mha-3195939 (describing the Pratibimb software, developed by I4C, used to map mule accounts and suspect locations).

ISSN: 2582-6433

difficulty remains in distinguishing between an individual who knowingly facilitates cybercrime and an individual whose account is used without the requisite criminal knowledge. The expression "money mule" does not itself resolve this distinction, while the same financial transaction may involve persons possessing substantially different degrees of culpability.

The principal research gap identified by this article is therefore the absence of a sufficiently clear analytical distinction between account involvement and criminal culpability. Contemporary cybercrime enforcement increasingly relies upon financial intelligence, transaction tracing and identification of accounts linked to fraudulent transactions. These mechanisms are essential for identifying criminal networks, but the identification of an account holder does not necessarily answer the separate question of whether that person possessed the mens rea required for criminal liability. The problem becomes particularly significant where individuals claim that they provided their accounts for a small financial benefit without knowing that the accounts would be used for cyber fraud.

The article therefore proposes a Culpability–Mens Rea Framework for analysing money-mule liability. Under this framework, criminal responsibility should be assessed through the interaction of three elements: (i) the conduct of the account holder, (ii) the degree of culpability established by the evidence, and (iii) the mental element required by the specific offence charged.

The proposed framework distinguishes five categories. An unauthorised account holder has no voluntary participation and should not incur criminal liability merely because the account appears in the financial trail. An unwitting money mule may voluntarily provide an account but lack knowledge of its criminal purpose. A negligent money mule may fail to exercise reasonable caution, but negligence should not automatically constitute criminal liability where the relevant offence requires knowledge or intention[25]. A reckless or deliberately blind participant occupies an intermediate position where suspicious circumstances exist but the person continues to participate while avoiding knowledge of the underlying activity. Finally, a knowing and intentional money mule deliberately facilitates the movement of criminal proceeds with the requisite awareness and therefore presents the strongest basis for criminal liability.

[25] Shiv Kumar v. State of Madhya Pradesh, (2022) 9 SCC 676 (negligence or failure to make inquiries does not, without more, satisfy the "reason to believe" standard).

ISSN: 2582-6433

The proposed framework can be expressed as:

Proved conduct + degree of culpability + statutory mens rea = criminal liability

This approach does not seek to create an exemption for persons who knowingly facilitate cybercrime. Rather, it seeks to ensure that enforcement is directed towards culpable participation rather than mere financial association. The framework also recognises that the required mental element differs according to the offence invoked and that suspicion, negligence, "reason to believe" and actual knowledge should not automatically be treated as legally identical[26].

The framework consequently attempts to reconcile two competing objectives: effective disruption of cybercrime networks and principled attribution of individual criminal responsibility. It provides a basis for evaluating whether Indian law can adequately distinguish the unwitting account holder from the deliberate financial facilitator and identifies the need for greater doctrinal clarity in the treatment of money-mule liability.

6. CONCLUSION

Money mules have become an important component of cyber-enabled financial crime because they provide the financial channels through which fraudulent proceeds can be received, transferred and withdrawn. The recent statewide enforcement operation in Tamil Nadu, resulting in the arrest of 837 persons connected with mule-account investigations, demonstrates the scale of the problem and the necessity of disrupting the financial infrastructure supporting cybercrime.

However, effective enforcement must be accompanied by precise attribution of criminal responsibility. The central argument of this article is that the use of a person's bank account in a cybercrime transaction should not, by itself, establish criminal liability. A financial trail can demonstrate the movement of money, but criminal responsibility additionally requires an assessment of the conduct and mental state of the individual in accordance with the specific offence charged.

The distinction between unauthorised account holders, unwitting money mules, negligent participants, reckless or deliberately blind participants and knowing facilitators is therefore significant. In particular, the law should distinguish mere negligence or suspicion from the knowledge, intention or "reason to believe" required by the applicable statutory provision. At the same time, individuals who knowingly and deliberately facilitate the movement of criminal

[26] Trimbak v. State of M.P., AIR 1954 SC 39.

ISSN: 2582-6433

proceeds should not be shielded merely by characterising themselves as intermediaries.

The proposed Culpability–Mens Rea Framework provides a means of addressing this tension. It places the person's proved conduct, degree of culpability and the statutory mental element at the centre of the inquiry. Such an approach can strengthen cybercrime enforcement while reducing the risk of imposing criminal liability solely on the basis of account ownership or financial association.

Ultimately, the challenge is not whether money mules should be prosecuted, but how the law should distinguish the unwitting intermediary from the culpable facilitator. A principled approach to money-mule liability must therefore ensure that financial tracing serves as the starting point of investigation, rather than becoming a substitute for proof of criminal mens rea.

References

Statutes

1. Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
2. Information Technology Act, No. 21 of 2000, India Code (2000).
3. Prevention of Money-Laundering Act, No. 15 of 2003, India Code (2003).
4. Indian Penal Code, No. 45 of 1860, India Code (1860) (repealed 2024).

Cases

5. Vijay Madanlal Choudhary v. Union of India, (2022) SCC OnLine SC 929 (India).
6. Pavana Dibbur v. Directorate of Enforcement, (2023) SCC OnLine SC 1586 (India).
7. Shiv Kumar v. State of Madhya Pradesh, (2022) 9 S.C.C. 676 (India).
8. S.D. Shabuddin v. State of Telangana, 2025 INSC 999 (India).
9. Trimbak v. State of Madhya Pradesh, AIR 1954 SC 39 (India).
10. Mohan Lal v. State of Maharashtra, (1979) 4 S.C.C. 751 (India).
11. Srinivas Mall Bairoliya v. Emperor, AIR 1947 PC 135 (India).
12. State of Maharashtra v. Mayer Hans George, AIR 1965 SC 722 (India).

Books

13. K.D. Gaur, *Textbook on the Indian Penal Code* (6th ed. 2016).

ISSN: 2582-6433

International Reports

14. Fin. Action Task Force, *Professional Money Laundering* (2018), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf [https://perma.cc/xxxx-xxxx].
15. Fin. Action Task Force, Interpol & Egmont Grp., *Illicit Financial Flows from Cyber-Enabled Fraud* (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf [https://perma.cc/xxxx-xxxx].

Government & Regulatory Materials

16. Reserve Bank of India, Circular No. RPCD.CO.RRB.AML.BC.No.40/03.05.33(E)/2010-11, *Operation of Bank Accounts & Money Mules* (Dec. 24, 2010).
17. *National Cybercrime Reporting Portal*, Gov't of India, https://cybercrime.gov.in/ (last visited Aug. 30, 2026).

News Sources / Websites

18. *Tamil Nadu Cops Go on "Mule Hunt", Arrest 837 Account Holders in Two-Day Statewide Drive*, DT Next (Aug. 2026), https://www.dtnext.in/news/tamilnadu/837-mule-account-holders-facilitating-cyber-cons-arrested-in-tamil-nadu.
19. *RBI Asks Banks to Collaborate with MuleHunter.AI to Find Mule Accounts*, Bus. Standard (Dec. 6, 2024), https://www.business-standard.com/finance/news/rbi-asks-banks-to-collaborate-with-mulehunter-ai-to-find-mule-accounts-124120600623_1.html.
20. Press Trust of India, *'Samanvaya' Portal for Data Exchange Among Police Forces on Cyber Criminals' Activities*, Deccan Herald, https://www.deccanherald.com/india/samanvaya-portal-for-data-exchange-among-police-forces-on-cyber-criminals-activities-mha-3195939 (last visited Aug. 30, 2026).
21. Fed. Bureau of Investigation, *Money Mules*, https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/money-mules (last visited Aug. 30, 2026).