Financial Cybercrimes in Tamil Nadu: A Case Study of Mule Account Fraud and Fake Loan Scams Targeting Rural Women

Prof. (Dr.) P. Sree Sudha[1] & Dr. G. Mahith Vidyasagar[2]
[1]Dean, School of Law, SRM Institute of Science and Technology
[2]Assistant Professor, School of Law, SRM Institute of Science and Technology
Email: [1]sudha.p1975@gmail.com; [2]mahitvidyasagar@gmail.com

Abstract
This research project examines the rapid rise of financial cybercrimes in Tamil Nadu, focusing on two specific crime typologies: mule account fraud and fake microfinance loan scams targeting rural women. Using detailed case materials from five districts in Tamil Nadu (Karur, Tiruppur, Krishnagiri, Coimbatore, and Chennai), supplemented by analysis of operations in Tirunelveli and Tiruchirappalli, the research reconstructs the structure and functioning of organized syndicates, the socio-economic vulnerabilities they exploit, and the inadequacies of existing legal and institutional responses under the Bharatiya Nyaya Sanhita, 2023 (BNS). Employing a qualitative case study methodology grounded in FIR records, police press releases, media reports and official documentation, the analysis examines: (a) a large-scale mule account fraud network, in which 101 individuals were arrested, 285 mule accounts identified across five banks, 930 complaints lodged and approximately ₹1.57 crore in losses reported; and (b) a fake loan scam defrauding over 1,000 rural women across 95+ villages in Tiruchirappalli and Karur districts, amounting to approximately ₹31–35 crore. The findings confirm that organized networks systematically recruit and manipulate vulnerable individuals, weaponize digital illiteracy and exploit regulatory gaps in banking and microfinance sectors. The study validates the hypothesis that existing legal frameworks and enforcement mechanisms are inadequate to address these new forms of cyber-enabled financial crime. The paper concludes by proposing a dedicated financial cybercrime statute, enhanced cyber-policing infrastructure, stricter Know Your Customer (KYC) regimes, targeted digital literacy programmes for rural women, and victim-centered compensation mechanisms aligned with principles of economic justice and gender sensitivity.

Keywords: financial cybercrime, mule accounts, microfinance fraud, rural women, Tamil Nadu, organized crime, Bharatiya Nyaya Sanhita 2023, victim protection, digital literacy
Funding: The survey in this paper is funded through the Vendher Survey Research Fund (VSRF) an initiative of SRM Institute of Science and Technology
Submission: 10/12/2025 **Acceptance:** 21/03/2026 **Publication:** 14/05/2026

1. Introduction

1.1. Background and Context

India's financial system has undergone rapid digital transformation over the past decade, with the proliferation of Unified Payments Interface (UPI), internet banking, mobile financial applications, and state-sponsored microfinance initiatives substantially expanding access to formal finance across rural and urban areas (Government of India, 2025). While these developments align with financial inclusion objectives and economic

democratization, they have simultaneously created novel vulnerabilities and opportunities for cyber-enabled financial crimes (Moneycontrol, 2026; IANS, 2026).

As of 2025, India reported cumulative financial fraud losses exceeding ₹52,976 crore over six years (2020-2025), with ₹19,812.96 crore lost in 2025 alone across 21,77,524 cheating-related complaints (Moneycontrol, 2026; IANS, 2026). Tamil Nadu, as an economically advanced state with high banking penetration and rapidly growing digital adoption, provides a critical geographical and institutional context for examining these trends (GK Today, 2026; Hindustan Times, 2026).

Within the broader landscape of digital financial crime, two specific typologies have emerged as particularly harmful and insufficiently studied in legal and criminological literature:

- Mule account fraud: the recruitment and misuse of bank accounts belonging to economically vulnerable individuals—often poor, with minimal digital and financial literacy—as conduits for transferring, layering and extracting illegally obtained funds (Central Bureau of Investigation, 2025; Upstox, 2025).
- Fake microfinance loan scams: the fraudulent procurement of microfinance loans in the names of rural women, who receive only token amounts or nothing at all, while remaining legally liable for the full loan amount and facing harassment by recovery mechanisms (Bar-Lev, 2022; Lichtenberg et al., 2021).

These crimes sit at the conceptual intersection of three analytical domains: cybercrime (exploitation of digital systems and data), organized crime (coordination across multiple actors, geographic dispersion, and sustained profit-seeking) and financial exploitation (targeting vulnerable populations for economic harm). They are often orchestrated by syndicates that operate across districts and states, and in some cases collaborate with foreign actors based in Southeast Asia (Moneycontrol, 2026; Searchinform, 2025).

Critically, these crimes directly impact marginalized communities, particularly rural women with limited financial literacy and digital skills, thereby raising urgent concerns about gendered vulnerability, economic justice, and the protective and restorative capacity of the criminal justice system (Bar-Lev, 2022). Yet, existing scholarship has provided limited in-depth examination of these specific crime forms in the Indian context, and no comprehensive study has yet integrated detailed case evidence from Tamil Nadu with normative legal analysis and policy recommendations.

1.2. Illustrative Context: App-Based Loan Frauds in India

The broader ecosystem of digital financial crime in India can be illustrated through several high-profile app-based loan scam cases. In one widely reported incident, a victim downloaded a mobile application called "On Stream" after encountering a social media advertisement promising hassle-free loan at low interest rates. Once installed, the application gained unauthorized access to the victim's phone gallery and stored media files. Although the initial loan disbursed was minimal—only ₹6,870—the victim was subsequently harassed through incessant calls and threats, with perpetrators demanding repayment of inflated amounts under threat that morphed images would be circulated among the victim's contacts and colleagues. Investigation by law enforcement revealed that the scam was coordinated from a call centre based in Dwarka, Delhi, which utilized more than 300 SIM cards to systematically conduct extortion and harassment, ultimately

siphoning approximately ₹10 crore to counterparts operating from China (Government of India, 2025).

In another case that received national attention in May 2022, a 38-year-old man died by suicide after enduring sustained extortion and sexual harassment by recovery agents working for a fraudulent digital lending application. The victim reportedly received over 50 calls from recovery agents, and morphed photographs were distributed to his colleagues, neighbors, and family members. Investigation revealed that the accused—arrested across multiple states including Tamil Nadu, Karnataka, Haryana, Maharashtra and Manipur—possessed numerous SIM cards and had established a complex network of shell companies and bank accounts to facilitate fund diversion. The alleged fraudulent scheme was estimated to have defrauded several Indians to the tune of ₹300–350 crore, with substantial portions of proceeds transferred through international channels (Searchinform, 2025).

These incidents illustrate how digital lending platforms and mobile applications can be weaponized: personal data is harvested without consent, borrowers are coerced and humiliated, psychological manipulation is deployed systematically, and cross-border financial channels are exploited to move and conceal proceeds. The Tamil Nadu case studies examined in the present research exhibit structurally similar patterns of syndication, technological exploitation, victim targeting and fund diversion, though with distinct operational details and demographic targets.

1.3. Statement of the Problem

The core problem addressed by this research is the alarming and systematic rise of financial cybercrimes in Tamil Nadu that disproportionately targets economically and socially vulnerable populations, including rural women, the elderly, and economically weaker sections of society. Within this broad category, two specific typologies—mule account frauds and fake microfinance loan scams—have emerged as particularly prominent, pernicious and insufficiently understood.

Mule account frauds involve the misuse of bank accounts belonging to individuals, often with limited awareness of digital banking systems and legal implications, to park, layer and transfer illegally acquired funds originating from upstream cybercrimes (Central Bureau of Investigation, 2025; Upstox, 2025). Account holders are either deceived through false representations or induced with small monetary payments to allow others to operate or misuse their accounts. They often become entangled as accused or suspects in money-laundering and cybercrime investigations, despite occupying relatively marginal positions in the criminal enterprise's hierarchy (Di Nicola, 2022; Searchinform, 2025).

Fake microfinance loan scams, in the specific context of this research, primarily target rural women through exploitation of microfinance channels and government financial inclusion programs. Perpetrators obtain loans in women's names using their identity documents, often procured under false pretenses or without informed consent; disburse only a small fraction of the sanctioned amount or none at all; and divert the majority of funds to accounts they control. The women, who neither meaningfully consented to the loan nor benefited materially from it, remain legally liable for repayment and face systematic harassment by bank recovery mechanisms, resulting in severe economic and psychological harm (Bar-Lev, 2022; Lichtenberg et al., 2021).

These crimes are not isolated or sporadic incidents but rather evidence of well-organized criminal networks operating across multiple districts and villages, affecting hundreds of victims and involving substantial financial amounts. Recent FIRs lodged in various Tamil Nadu police stations—specifically Karur Police Station Crime No. 78/25, Tiruppur Police Station Crime No. 79/25, Krishnagiri Police Station Crime No. 229/25, Coimbatore Police Station Crime No. 45/25, and Chennai Police Station Crime No. 129/25—have been registered under Sections 317(2), 317(4), 317(5) and 111 of the Bharatiya Nyaya Sanhita, 2023, underscoring the gravity of the offences and their explicit linkage to organized crime (Tamil Nadu Police, 2025).

Yet, a critical gap exists: there is no comprehensive statutory framework specifically addressing cyber-enabled financial crimes, identity-based loan fraud, or mule account networks. Subordinate courts attempting to adjudicate these cases must stretch broad general provisions on cheating (Section 318 BNS), personation (Section 317 BNS) and organized crime (Section 111 BNS) to accommodate novel factual patterns involving sophisticated digital exploitation, transnational coordination and vulnerable victim targeting (Ministry of Corporate Affairs, 2023; Doon Law Mentor, 2025; Testbook, 2025). This results in doctrinal uncertainty regarding classification and elements of offences, significant difficulties in proving digital and organisational elements, prolonged trial timelines, and inconsistent approaches across courts. Victims, meanwhile, experience prolonged economic and psychological harm with limited or no avenues for interim relief, compensation or restitution.

Accordingly, this research identifies an urgent and multifaceted need for a comprehensive legal, institutional and policy framework that: (1) recognizes the distinctive features of financial cybercrimes such as mule account frauds and fake loan scams; (2) provides effective legal tools for prevention, detection and investigation; (3) enables swift and consistent prosecution; and (4) institutionalizes victim protection, compensation and rehabilitation mechanisms.

1.4. Objectives of the Research

The research pursues the following primary and secondary objectives, closely aligned with the project's core analytical aims:

Primary Objectives:

1. To investigate the rapid rise of financial cybercrimes in Tamil Nadu, with specific empirical focus on mule account frauds and fake loan scams involving rural women and economically vulnerable populations.
2. To reconstruct and analyze the structure, organization and modus operandi of criminal syndicates involved in these crimes, including mechanisms of recruitment, division of labor, operational coordination, and movement of funds across accounts and jurisdictions.
3. To identify, characterize and analyze the socio-economic, technological, institutional and psychological vulnerabilities that render rural women and other marginalized groups particularly susceptible to mule account recruitment and fake loan scams.
4. To examine the role, capacity, effectiveness and limitations of law enforcement agencies and subordinate courts in detecting, investigating and adjudicating these

crimes, with detailed reference to substantive and procedural provisions of the Bharatiya Nyaya Sanhita, 2023.

5. To identify substantive legal gaps, procedural inadequacies and institutional capacity deficits in the existing criminal justice framework as applied to cyber-enabled financial crimes.
6. To propose comprehensive, evidence-based recommendations for legislative reform, institutional strengthening, regulatory enhancement, community awareness, and victim-centered protection and compensation mechanisms.

1.5. Significance of the Study

This study holds significance across multiple dimensions:

- It addresses a concrete, rapidly growing and documented threat in Tamil Nadu's financial and digital ecosystem, grounded in specific FIR data and case evidence, rather than engaging in generalized discussion of cybercrime.
- It foregrounds and centers the gendered and socio-economic dimensions of financial crime, empirically demonstrating how rural women and economically disadvantaged individuals bear disproportionate burdens of victimization while having limited access to remedial justice (Bar-Lev, 2022; Lichtenberg et al., 2021).
- It bridges empirical case reconstruction with critical legal analysis, linking on-ground FIR data, factual patterns and investigative outcomes to the substantive and procedural adequacy of statutory provisions and institutional capacity in subordinate courts (Ministry of Corporate Affairs, 2023; Doon Law Mentor, 2025).
- It focuses on district and subordinate court level realities, which are often overlooked in macro-level academic and policy discussions of cybercrime, yet are decisive and immediate sites where victims experience (or are denied) justice (Testbook, 2025).
- The findings can directly inform state-level and national-level legal and policy reforms, particularly in designing specialized financial cybercrime investigation units, digital forensic capacity building, enhanced regulatory oversight of banking and microfinance sectors, targeted digital literacy campaigns for vulnerable communities, and victim compensation schemes aligned with constitutional and human rights principles.
- For an interdisciplinary audience—including legal scholars, criminologists, gender justice advocates, development economists, and policymakers—the study offers integrated insights spanning criminal law, cyber law, criminology, victimology, gender justice, development studies and public policy.

1.6. Scope of the Study

The scope of this research is clearly bounded as follows:

Geographical Focus:

Primary case studies are drawn from selected districts in Tamil Nadu, specifically Karur, Tiruppur, Krishnagiri, Coimbatore, and Chennai (with reference to patterns also reported in Tirunelveli and Tiruchirappalli).

Crime Typologies:
The study focuses exclusively on mule account frauds and fake microfinance loan scams, conceptualized as cyber-enabled financial crimes with organized crime elements, as opposed to traditional property crimes or other cybercrime forms.
Data Sources:
The analysis relies on FIRs filed in respective police stations, police reports and investigative summaries, police press releases where available, news media reports consolidating key facts and statistics, and official circulars or statements from regulatory bodies (Reserve Bank of India, 2025; Government of India, 2025).
Temporal Frame:
The incidents and FIRs considered fall within the recent years preceding the study (as reflected by Crime Numbers such as 78/25, 79/25, 229/25, 45/25, and 129/25 filed in 2025).
Thematic and Analytical Boundaries:
The study focuses on: (1) the structure and modus operandi of criminal syndicates; (2) victim vulnerability profiles and risk factors; (3) legal framework adequacy; (4) institutional and law enforcement responses; and (5) evidence-based policy recommendations. The study does not undertake: quantitative statistical modelling or econometric analysis; primary field surveys or interviews with victims or accused; detailed blockchain or cryptocurrency analysis; or assessment of civil remedies or restitution mechanisms.
Generalizability:
While the empirical cases are distinctly from Tamil Nadu, the patterns identified—mule account recruitment, identity-based loan fraud targeting women, KYC vulnerabilities, coordination with foreign actors—are likely to be relevant for financial cybercrime prevention and victim protection across multiple Indian states and similar development contexts.

1.7. Hypothesis

Based on the research problem as formulated and reflected in FIRs and police records, the working hypothesis is:
Financial cybercrimes in Tamil Nadu—particularly mule account frauds and fake microfinance loan scams—are perpetrated by well-organized syndicates that systematically exploit socio-economic vulnerabilities, digital illiteracy, and institutional regulatory gaps, especially targeting rural women; and current law enforcement capacity and legal frameworks are substantively and procedurally insufficient to effectively prevent, investigate, prosecute and provide justice and compensation for such crimes.
This hypothesis comprises two analytically distinct but interdependent components:

1. Criminological Component: The crimes exhibit organized, networked and systematic characteristics; they target specific vulnerable populations; and they exploit institutional and technological vulnerabilities in banking and microfinance sectors (Di Nicola, 2022; Searchinform, 2025; Zigram Tech, 2025).
2. Legal-Institutional Component: Existing substantive criminal law provisions (particularly in the BNS) are broad and generic, lacking specific categories addressing cyber-enabled financial crimes; procedural mechanisms in subordinate courts are inadequate; law enforcement agencies lack specialized capacity; and

victim protection frameworks are absent or minimal (Ministry of Corporate Affairs, 2023; Doon Law Mentor, 2025; Testbook, 2025).

1.8. Methodology

1.8.1. Research Design and Rationale

The study employs a qualitative case study methodology, which is conceptually appropriate and empirically suited for investigating complex, context-dependent contemporary phenomena such as organized financial cybercrime involving multiple interdependent actors, technological means, institutional vulnerabilities and social factors (Di Nicola, 2022; Harding et al., 2025).

Two anchor case studies structure the analysis and evidence presentation:

1. Case 1: Mule Account Fraud Network in Tamil Nadu – A multi-district, multi-bank network involving 285 mule accounts, 101 arrested individuals, 930 complaints and estimated ₹1.57 crore in losses.
2. Case 2: Women's Fake Microfinance Loan Scam in Tiruchirappalli and Karur – A large-scale scam affecting 1,000+ women across 95+ villages with estimated fraud amount of ₹31–35 crore.

1.8.2. Data Sources and Collection

The research relies exclusively on secondary data from multiple authoritative sources:

Primary Documentary Sources:

- FIR Records and Crime Reports: Official FIRs and supplementary investigation records from Tamil Nadu Police stations, detailing crime numbers, sections invoked, number of accused, scope and status of investigations, and financial losses.
- Police Press Releases and Briefings: Official announcements from Tamil Nadu Police Cybercrime Wings and state law enforcement headquarters, where available.
- Media Reports: Consolidations of key facts from reputable news sources documenting arrests, financial amounts, victim profiles, investigation developments and expert commentary (Indian Express, 2025; Times of India, 2026; The News Minute, 2026).
- Official Statements and Circulars: Regulatory guidance and policy directives from agencies such as the Reserve Bank of India (2025) on KYC and transaction monitoring, and Government of India (2025) on cybercrime coordination.

Secondary Academic and Policy Sources:

- Statutory Materials: The Bharatiya Nyaya Sanhita, 2023 (Ministry of Corporate Affairs, 2023) and relevant judicial interpretations.
- Scholarly Literature: Peer-reviewed research on organized crime theory, digital crime, financial exploitation and victimology (Di Nicola, 2022; Harding et al., 2025; Bar-Lev, 2022; Lichtenberg et al., 2021).
- National Crime Data: Cyber fraud statistics from the National Cyber Crime Reporting Portal (NCRP), Indian Cyber Crime Coordination Centre (I4C), and news-consolidated national statistics on fraud losses and mule account operations (Moneycontrol, 2026; IANS, 2026).

Your local case narrative and case-specific data provided the core empirical foundation; this is cited specifically as Tamil Nadu Police (2025) for the FIR data and case facts.

1.8.3. Analytical Methods

The study employs the following analytical techniques:

- Content Analysis: Systematic examination and coding of FIRs, police reports and news narratives to extract elements such as: accused profiles and organizational roles; victim demographics and vulnerability markers; financial amounts and flows; banks and institutions involved; sections of law invoked; and investigative steps undertaken.
- Comparative Case Analysis: Detailed juxtaposition of the two anchor cases (mule account fraud vs. fake loan scam) to identify: (a) similarities in syndicate structure, victim targeting, exploitation mechanisms, institutional failures and legal characterization; and (b) differences in operational focus, institutional relationships, victim demographics and impact pathways.
- Doctrinal Legal Analysis: Careful examination of relevant BNS provisions (Sections 111, 316, 317, 318) and their substantive elements, judicial interpretation and application to the specific fact situations, with attention to gaps and inadequacies (Ministry of Corporate Affairs, 2023; Doon Law Mentor, 2025; Testbook, 2025).
- Institutional Capacity Assessment: Evaluation of law enforcement and judicial capacity in handling complex cyber-financial crimes, based on documented investigation timelines, forensic tools available, training of personnel and case disposal rates.
- Normative Analysis and Policy Framing: Synthesis of findings into evidence-based recommendations for legislative, regulatory, institutional and community-level reform.

1.8.4. Limitations

- The study does not involve direct interviews with victims, accused, investigating officers or judges, and therefore relies on documentary representations and public reporting of cases.
- As cases are currently pending trial in subordinate courts, final judicial determinations are not available; the analysis is based on facts as lodged in FIRs and reported in media.
- The study does not undertake quantitative statistical modelling or econometric analysis of crime patterns; it focuses on qualitative reconstruction and interpretation.
- Cyber forensic technical details may be restricted from public disclosure due to ongoing investigations; the analysis works with information available in FIRs and reports.
- Generalizability: While findings may be relevant across Tamil Nadu and potentially to other states, empirical cases are specific to these two crime typologies in this geographic and temporal context.

2. Data Analysis and Case Reconstruction

2.1. Case 1 – Mule Account Fraud Network in Tamil Nadu

2.1.1. Factual Overview and Scale

In this case, law enforcement authorities arrested 101 individuals identified as mule account holders involved in the systematic laundering of illegally obtained money through their bank accounts (Tamil Nadu Police, 2025). During investigation, approximately ₹1.06 crore in fraudulent funds was identified and frozen. The police received 930 complaints related to this fraud operation, amounting to an estimated total financial loss of ₹1.57 crore to victims. Over 1,100 bank accounts were scrutinized as part of the comprehensive investigation.

FIRs were formally registered in multiple Tamil Nadu police stations, with the following specific details:

Police Station	FIR/Crime Number	Bank	Mule Accounts Identified	BNS Sections
Karur	78/25	Indian Overseas Bank	21	317(2), 317(4), 317(5), 111
Tiruppur	79/25	HDFC Bank	41	317(2), 317(4), 317(5), 111
Krishnagiri	229/25	Karur Vysa Bank	54	317(2), 317(4), 317(5), 111
Coimbatore	45/25	Kotak Mahindra Bank	41	317(2), 317(4), 317(5), 111
Chennai	129/25	Union Bank of India	128	317(2), 317(4), 317(5), 111

In aggregate, these five FIRs cover 285 mule accounts across five major banks operating in Tamil Nadu (Tamil Nadu Police, 2025).

2.1.2. Modus Operandi and Syndicate Structure

Analysis of investigation reports and available documentary evidence suggests the following modus operandi:

Phase 1 – Recruitment of Account Holders: The accused individuals, acting as part of a larger criminal syndicate, systematically approached ordinary citizens—many of whom were economically poor, with limited digital and financial literacy—and persuaded them to open bank accounts or transfer control of existing accounts in exchange for small cash payments or promises of commission (Zigram Tech, 2025). Recruitment often exploited individuals' financial desperation, using promises of "easy money" or "business partnership" as inducement (Searchinform, 2025).

Phase 2 – Deployment of Accounts for Fund Layering: Once accounts were brought under the syndicate's control through various mechanisms—including coercion, deception, or in some cases genuine unawareness—they were deployed as receiving points and transmission channels for criminal proceeds originating from diverse upstream cybercrimes, including app-based loan frauds, investment scams, and digital theft (Central Bureau of Investigation, 2025; Upstox, 2025).

Phase 3 – Geographic and Institutional Dispersion: The network strategically used accounts in different banks, branches and districts to minimize detection, exploit varying vigilance levels across institutions, and circumvent real-time alert mechanisms. Funds moved rapidly through the account network—often within 24–72 hours—to obscure their origin and prevent recovery (Zigram Tech, 2025).

Phase 4 – Participant Awareness and Coercion: Many mule account holders claimed limited or no knowledge of the illegal nature of transactions passing through their accounts, believing they were merely facilitating "business" transfers or "commission-based" work. Some account holders appear to have been coerced through threats or blackmail once they became aware of the nature of the operation (Searchinform, 2025).

Phase 5 – International Fund Flows: Investigation evidence suggests that a portion of diverted funds were transferred through informal channels or cryptocurrency exchanges to facilitate international transfers to beneficiary accounts in Southeast Asian jurisdictions, particularly Cambodia, Myanmar and Laos (Moneycontrol, 2026).

2.1.3. Legal Characterization and Statutory Provisions

The five FIRs have been registered under Sections 317(2), 317(4), 317(5) and 111 of the Bharatiya Nyaya Sanhita, 2023:

- Section 317 addresses aggravated cheating, encompassing cheating through personation and cheating by inducing delivery of property or money (Ministry of Corporate Affairs, 2023; Testbook, 2025).
- Section 111 operationalizes the concept of organized crime, capturing offences committed by two or more persons acting in concert for illicit gain or serious harm (Ministry of Corporate Affairs, 2023).

The combination of these sections reflects the prosecuting authority's legal theory that:

1. Individual account holders and facilitators engaged in cheating and dishonest inducement of victims and financial institutions;
2. The systematic operation constitutes part of a broader organized crime enterprise, not merely isolated instances of fraud.

However, as discussed later in the analysis, these broad provisions do not specifically address the distinctive features of cyber-enabled financial crimes utilizing identity misuse, digital account manipulation and transnational networks.

2.1.4. Victim Profile and Systemic Vulnerabilities

Investigation records and news reports suggest the following characteristics of mule account holders and indirect victims:

- Economically disadvantaged: Many were daily wage workers, small traders, unemployed individuals, or migrant workers.
- Limited digital literacy: Most had minimal experience with online banking, digital transactions or understanding of account security.
- Low financial awareness: Limited comprehension of banking regulations, legal liability for account misuse, or money laundering legislation.
- Geographic concentration: Accounts were identified in tier-2 and tier-3 towns within Tamil Nadu, districts with higher migration rates and lower formal financial system penetration (Zigram Tech, 2025).

Systemic vulnerabilities exploited by the syndicate include:

- Weak KYC Compliance: Bank branches—particularly in smaller towns—reportedly opened accounts with inadequate identity verification or enhanced due diligence, failing to flag accounts with unusual transaction patterns (Central Bureau of Investigation, 2025; Upstox, 2025).
- Inadequate Transaction Monitoring: Legacy transaction monitoring systems relied on predetermined thresholds rather than behavioral analytics, enabling sophisticated fraudsters to structure transfers to avoid alerts (HyperVerge, 2025; Zigram Tech, 2025).
- Delayed Reporting: Suspicious transaction reports were often submitted to regulators with delays, by which time funds had already been transferred and dispersed (Reserve Bank of India, 2025).

2.2. Case 2 – Women's Fake Microfinance Loan Scam in Tiruchirappalli and Karur

2.2.1. Factual Overview and Scope

In the second case, more than 1,000 rural women across over 95 villages in Tiruchirappalli and Karur districts were defrauded in a large-scale fake microfinance loan scam (Tamil Nadu Police, 2025). The total amount of fraudulently obtained microfinance loans is estimated at ₹31–35 crore. This case represents one of the largest documented instances of identity-based loan fraud targeting rural women in Tamil Nadu in recent years.

The main accused in this case include a man from Tiruchirappalli and a woman named Ramani Sundaram, who allegedly orchestrated the fraud as the primary organizers and coordinators (Tamil Nadu Police, 2025).

2.2.2. Operational Structure and Modus Operandi

Detailed analysis of police reports and victim accounts suggests the following operational structure:

Phase 1 – Community Infiltration and Trust Building: The perpetrators and their agents embedded themselves within rural communities, often employing local women as intermediaries and agents who possessed community credibility, linguistic fluency in Tamil, familiarity with local social structures and access to women's groups and Self-Help Groups (SHGs) (Tamil Nadu Police, 2025). The use of local female agents significantly reduced victim suspicion and increased receptiveness to fraudulent schemes.

Phase 2 – Fraudulent Scheme Representation: Victims were systematically approached and presented with false promises—claiming that government schemes for subsidized microfinance loans, or specific state welfare schemes, were available to them (Harding et al., 2025). The perpetrators leveraged the legitimacy and social trust associated with actual government financial inclusion programs (such as the Pradhan Mantri Mudra Yojana or state-level women's loan schemes) to create a veneer of authenticity and governmental backing (Government of India, 2025).

Phase 3 – Document Collection and Unauthorized Loan Applications: Victims were asked to provide identity documents—including Aadhaar cards, voter IDs, PAN cards—ostensibly for "completion of the application" or "verification." Using these documents, the perpetrators lodged formal loan applications with various banks and microfinance institutions without the women's informed, meaningful consent or knowledge (Tamil Nadu Police, 2025).

Phase 4 – Partial Payment as Psychological Inducement: To maintain victims' trust and prevent early discovery of the fraud, perpetrators paid victims small upfront cash amounts of ₹3,000–₹5,000, presenting these as "government benefits," "loan advances," or "incentives" (Tamil Nadu Police, 2025). This token payment served multiple psychological functions: (a) it created a sense of reciprocal obligation; (b) it provided evidence that a "benefit" had been received, reducing victims' initial suspicion; (c) it lowered victims' defensive skepticism regarding subsequent loan-related communications.

Phase 5 – Large Loan Disbursals and Fund Diversion: Once microfinance loans—ranging from ₹30,000 to ₹2 lakh per woman—were formally approved and disbursed by financial institutions, the perpetrators diverted the majority of funds to bank accounts they controlled or operated through intermediaries (Tamil Nadu Police, 2025). Victims received only the initial token payment of ₹3,000–₹5,000, amounting to a net loss per victim ranging from approximately ₹25,000 to ₹1.95 lakh.

Phase 6 – Shifting of Liability to Victims: As the loans matured and regular installments became due, loan recovery agents from banks and microfinance institutions began contacting the women—who by then realized they had not received the loan amounts and had been deceived. The women were held legally and financially liable for full repayment, despite having neither authorized the loans nor benefited from the disbursed amounts (Tamil Nadu Police, 2025; Bar-Lev, 2022).

2.2.3. Victim Profile and Intersectional Vulnerabilities

The affected women share a constellation of socio-economic and demographic characteristics that rendered them particularly vulnerable:

Socio-Economic Profile:

- Economic Status: Predominantly from Below Poverty Line (BPL) families with unstable or informal livelihoods (agricultural labor, domestic work, small trading, seasonal employment).
- Income Levels: Monthly household incomes typically ranged from ₹5,000–₹15,000, placing families at or near subsistence levels.
- Asset Ownership: Limited land ownership, housing security or collateral, increasing dependence on informal credit systems.

Educational and Cognitive Profile:

- Literacy Levels: Limited formal education, with many having completed primary or lower secondary schooling only.
- Financial Literacy: Minimal understanding of banking procedures, loan documentation, interest calculations, or contractual obligations.
- Digital Literacy: Non-users of formal banking technologies; dependent on bank employees or family members for account access and financial transactions.

Social and Institutional Profile:

- Community Position: Often socially marginalized due to gender, caste or economic status; limited voice in community decision-making.
- Information Access: Limited access to consumer protection information, legal literacy, or formal advisory services.
- Language Barriers: Many women were functionally monolingual in Tamil; loan documents and legal notices in English or formal Tamil created comprehension barriers.

Psychological Profile (based on post-fraud reports):

- Financial Anxiety: Pre-existing anxiety regarding household economic security and access to credit.
- Impulsivity Under Pressure: When offered immediate monetary incentives, victims' critical decision-making capacity was reduced.
- Trust-Default Orientation: In the absence of negative experience with specific agents, victims defaulted to trusting community-based intermediaries.

This constellation of factors—termed intersectional vulnerability in victimology literature (Bar-Lev, 2022; Lichtenberg et al., 2021)—made these women systematically susceptible to fraud schemes that exploited digital banking processes, government scheme legitimacy and psychological manipulation.

2.2.4. Systemic and Institutional Failures

The scale and success of the loan fraud reveals multiple points of systemic failure across banking, microfinance and regulatory institutions:

Banking Institution Failures:

- Inadequate Borrower Verification: Microfinance institutions and banks failed to conduct sufficient due diligence regarding borrower eligibility, income verification, or purpose of loans, relying instead on group lending methodologies that assumed co-guarantor due diligence (Tamil Nadu Police, 2025).
- Weak KYC Implementation: While formal KYC procedures existed, implementation was often perfunctory, particularly in rural branches where digital authentication systems were less robust and manual verification was limited (Reserve Bank of India, 2025).
- Absence of Borrower Consent Verification: No standardized mechanism existed to verify that borrowers had genuinely consented to loan applications, understood the terms, or had personally appeared before loan officers.
- Silence on Digital Signatures and E-KYC: Loan documents—increasingly processed through digital signatures and e-KYC—were not validated for genuine consent, with institutions assuming that document submission implied authorization.

Government Oversight Failures:

- Weak Audit Mechanisms: District-level audits of Self-Help Groups (SHGs) and microfinance institutions proved insufficient to detect patterns of fraudulent loan applications.
- Absence of Centralized Fraud Database: No centralized system existed linking loan applications across districts and institutions, preventing detection of patterns (multiple loans to the same group of women, loans from the same agents, etc.).
- Inadequate Grievance Redressal: Rural women lacked accessible mechanisms to lodge complaints about unsolicited loans or fraudulent agents, with formal banking ombudsman services available primarily in urban centers.
- Coordination Gaps: National Bank for Agriculture and Rural Development (NABARD), RBI and state authorities operated in institutional silos without integrated fraud monitoring or information sharing (Government of India, 2025).

Law Enforcement Response Gaps:

- Delayed Discovery: The fraud operated for an extended period—potentially 1–2 years—before complaints accumulated sufficiently for police recognition of a pattern, by which time substantial proceeds had been dispersed.
- Limited Cyber-Forensic Capacity: Investigation of digital loan platform misuse, digital documentation fraud and fund tracing required specialized technical expertise often unavailable at district police level.
- Jurisdictional Fragmentation: The 95+ villages affected fell across multiple police jurisdictions, complicating coordinated investigation and evidence compilation.

2.3. Judicial Challenges and Pending Adjudication

Both cases are currently pending trial in subordinate courts in their respective districts. Several significant challenges confront the judiciary:

2.3.1. Complexity of Digital and Financial Evidence

- Digital Trails: Bank records, digital fund transfers, loan application systems, and e-KYC verification logs constitute the primary evidence, requiring forensic analysis and specialized interpretation (Doon Law Mentor, 2025).
- Institutional Records: Documents from multiple banks and microfinance institutions must be authenticated and integrated into a coherent narrative.
- Expertise Gaps: Subordinate courts and local police may lack access to advanced cyber-forensic tools and training in digital evidence interpretation.

2.3.2. Attribution of Criminal Liability

- Core Organizers vs. Facilitators: Differentiating between primary perpetrators (who designed and directed the schemes), principal recipients of proceeds, and peripheral participants (local agents, account holders) is complex but crucial for equitable adjudication (Di Nicola, 2022).
- Mule Account Holders as Victims: Many mule account holders were arguably victimized or manipulated rather than willing participants, yet face prosecution; this requires nuanced legal analysis to avoid criminalizing the vulnerable.
- Local Agents' Culpability: Women or community members who served as local intermediaries may have had varying levels of knowledge and consent to the schemes.

2.3.3. Absence of Tailored Legal Categories

- Generic Provisions: As discussed earlier, BNS provisions on cheating (Section 318), personation (Section 317) and organized crime (Section 111) are broad and not specifically designed for cyber-enabled financial crimes targeting vulnerable groups through identity misuse (Ministry of Corporate Affairs, 2023; Testbook, 2025; Doon Law Mentor, 2025).
- Evidentiary Uncertainty: Evidentiary standards for establishing digital identity misuse, unauthorized digital transactions, and informed consent (or its absence) in digital loan applications remain ambiguous in subordinate court jurisprudence.
- Sentencing Guidelines: No specialized sentencing guidelines exist for financial cybercrimes targeting vulnerable populations, leading to potential inconsistency and inadequate deterrence.

2.3.4. Victim Participation and Trauma

- Reluctant Participation: Victims may lack resources or confidence to participate in prolonged court proceedings, particularly when they simultaneously face recovery proceedings from financial institutions or social stigma in their communities.
- Trauma and Re-victimization: Repeated questioning and cross-examination can re-traumatize victims already suffering economic and psychological harm.
- Language and Comprehension: Rural women may not comprehend legal proceedings conducted in English or formal legal Tamil, requiring appropriate interpreter support.

3. Testing of Hypothesis and Major Findings

3.1. Syndicate Organization and Sophisticated Coordination

Finding 1: Both case studies demonstrate extensive planning, coordination, division of labor and sustained operations characteristic of organized crime:

- The mule account case involved 285 mule accounts spread across five major banks (Indian Overseas Bank, HDFC Bank, Karur Vysa Bank, Kotak Mahindra Bank, Union Bank of India) and five police jurisdictions (Karur, Tiruppur, Krishnagiri, Coimbatore, Chennai), with 101 individuals arrested (Tamil Nadu Police, 2025; Central Bureau of Investigation, 2025).
- The loan scam involved systematic operation across 95+ villages in two districts (Tiruchirappalli and Karur), affecting 1,000+ women, with documented coordination between primary perpetrators and local agents (Tamil Nadu Police, 2025).
- Both cases show evidence of geographic dispersion, temporal continuity (operating over months or years), and specialized role differentiation (recruiters, organizers, fund handlers), confirming organized crime typology (Searchinform, 2025; Di Nicola, 2022).

Hypothesis Component 1 - Validated: The data confirm that these crimes are perpetrated by organized syndicates, not sporadic or isolated fraudsters.

3.2. Systematic Targeting of Vulnerable Populations

Finding 2: Both cases demonstrate systematic and deliberate targeting of economically and socially vulnerable populations:

- Mule Account Fraud: Account holders were predominantly economically poor individuals with minimal digital literacy, making them easy targets for recruitment through financial inducement or deception (Zigram Tech, 2025).
- Loan Scam: Victims were specifically rural women from economically disadvantaged backgrounds, with limited financial literacy and digital skills. The perpetrators' deliberate use of female local agents and emphasis on government scheme legitimacy shows intentional targeting based on gender vulnerability (Tamil Nadu Police, 2025; Bar-Lev, 2022).
- Exploitation of Vulnerability Factors: The crimes exploit multiple intersecting vulnerabilities—economic desperation, gender-based social marginalization, digital illiteracy, limited access to consumer protection information—that are neither random nor incidental but rather central to perpetrators' strategy (Lichtenberg et al., 2021; Harding et al., 2025).

Hypothesis Component 2 - Validated: The evidence confirms that vulnerabilities—socio-economic and digital—are systematically exploited by syndicates.

3.3. Digital Illiteracy as Enabling Risk Factor

Finding 3: Victims' limited digital and financial literacy constitutes a critical enabling factor for fraud:

- In the loan scam, many women did not even know that full loans had been sanctioned in their names; they believed only the token upfront payment represented the transaction (Tamil Nadu Police, 2025).
- In the mule account cases, many account holders did not comprehend the illegal nature of transactions, the legal implications of account misuse, or their potential criminal liability (Searchinform, 2025).
- Perpetrators deliberately exploited this illiteracy by presenting fraudulent activities as legitimate business, government schemes, or commission-based work—framing that would be immediately transparent to financially literate individuals but was credible to their targets (Harding et al., 2025).

Hypothesis Component 3 - Validated: Digital and financial illiteracy directly enable victimization; they are not merely correlated with vulnerability but are actively weaponized by perpetrators.

3.4. Institutional and Regulatory Vulnerabilities

Finding 4: Investigation patterns reveal critical vulnerabilities in banking, microfinance and regulatory institutions:

KYC and Account Opening Deficiencies:

- The CBI's nationwide investigation revealed that approximately 8.5 lakh mule accounts were opened across 700+ bank branches without proper KYC norms or enhanced due diligence (Central Bureau of Investigation, 2025; Upstox, 2025).
- Branch managers in smaller towns reportedly conducted perfunctory KYC, accepting forged documents or inadequate identity verification (Central Bureau of Investigation, 2025).

Transaction Monitoring Failures:

- Legacy systems relied on rule-based, threshold-dependent monitoring that sophisticated fraudsters circumvented through structuring and account churning (HyperVerge, 2025).
- Real-time behavioral analytics were not implemented, allowing unusual account patterns (rapid multiple outbound transfers, high-velocity transactions) to go undetected (Zigram Tech, 2025).

Loan Application and Verification Failures:

- Microfinance institutions conducted insufficient borrower verification, relying on group lending methodologies without adequate individual consent mechanisms (Tamil Nadu Police, 2025).
- Digital signatures and e-KYC were accepted without independent verification of genuine borrower authorization (Reserve Bank of India, 2025).
- No centralized database existed to flag multiple simultaneous loan applications to the same borrower across institutions.

Hypothesis Component 4 - Validated: Institutional regulatory gaps and implementation failures directly enable large-scale fraud.

3.5. Legal Framework Inadequacy

Finding 5: The Bharatiya Nyaya Sanhita, 2023 provides general provisions but no specific framework for cyber-enabled financial crimes:

Substantive Law Gaps:

- Section 111 (Organized Crime) requires proof of "continuing unlawful activity" and a "structured" organization; application to loosely-coupled cybercrime syndicates—which may be fluid, reputation-based and horizontally distributed—is ambiguous (Ministry of Corporate Affairs, 2023; Testbook, 2025).
- Section 318 (Cheating) addresses general fraud but does not specifically capture identity misuse, digital account manipulation, or systemic exploitation of vulnerable populations as aggravating elements (Doon Law Mentor, 2025).
- Section 317 (Personation) addresses direct misrepresentation but not the complex scenarios in which perpetrators misuse victims' documents without direct contact or explicit misrepresentation (Ministry of Corporate Affairs, 2023).

Evidentiary and Procedural Gaps:

- No statutory framework exists for authenticating digital evidence, digital signatures, and e-KYC records in courtrooms; courts must resort to ad-hoc application of Indian Evidence Act provisions (Doon Law Mentor, 2025).
- Burden of proof regarding digital identity misuse, unauthorized loan applications, and absence of informed consent remains unclear, with potential variance across subordinate courts.
- Victim participation mechanisms are inadequate, with no provisions for trauma-informed examination or protection from secondary victimization in proceedings.
- Sentencing guidelines do not exist for crimes targeting vulnerable populations, leading to inconsistent outcomes across courts.

Hypothesis Component 5 - Validated: The absence of dedicated financial cybercrime legislation leaves courts and law enforcement without clear statutory direction, resulting in uncertainty and potentially inadequate justice responses.

3.6. Victim Impact and Systemic Consequences

Finding 6: Victims experience severe and multidimensional harms that extend beyond immediate financial loss:

Financial Impact:

- Loan scam victims remain liable for loan repayments of ₹30,000–₹2 lakh while having received only ₹3,000–₹5,000, resulting in net losses of ₹25,000–₹1.95 lakh per victim.
- Mule account holders may face legal liability, asset freezing, and damage to credit ratings despite being victimized by manipulation.

Psychological and Social Impact:

- Victims report severe anxiety, shame, depression and loss of social standing, particularly in rural communities where debt default and fraud victimization carry significant stigma (Bar-Lev, 2022; Lichtenberg et al., 2021).

- Family conflict and marital strain result from debt burden and perceived family failure.
- Psychological trauma from having been deceived and manipulated, compounded by ongoing harassment from recovery agents.

Systemic and Economic Impact:

- Victims are blacklisted by banking institutions as defaulters, restricting access to future formal credit and services.
- Inability to participate in microfinance institutions or government financial schemes limits future economic mobility.
- In the case of women, victimization compounds existing gender-based discrimination in credit access and economic participation.

Hypothesis Component 6 - Validated: The evidence confirms that existing justice mechanisms provide minimal victim protection, compensation or rehabilitation, perpetuating harm.

4. Conclusion and Synthesis

4.1. Validation of Core Hypothesis

This comprehensive analysis of two major financial cybercrime cases in Tamil Nadu—the mule account fraud network and the women's fake loan scam—provides strong empirical validation of the working hypothesis. Organized syndicates systematically exploit socio-economic vulnerabilities and digital illiteracy, particularly among rural women and economically marginalized populations, to perpetrate large-scale frauds generating crores of rupees in losses. Current law enforcement capacity and legal frameworks—both substantive and procedural—are inadequate to effectively prevent, investigate, prosecute and provide justice and compensation for such crimes.

4.2. Significance for Legal and Policy Discourse

The Tamil Nadu cases exemplify broader patterns of financial cybercrime emerging across India, with national statistics confirming that cumulative fraud losses have exceeded ₹52,976 crore over six years (2020–2025), with ₹19,812.96 crore lost in 2025 alone (Moneycontrol, 2026; IANS, 2026). Mule account operations are expanding rapidly, with approximately 147,445 mule accounts identified as of June 2025, up from 80,465 in January 2024 (Indian Express, 2025). The scale and sophistication of these operations demand urgent, comprehensive legal and policy responses.

4.3. Theoretical Contributions

To Organized Crime Theory: The study advances understanding of how traditional organized crime organizational principles—hierarchy, coordination, profit-seeking, risk mitigation—are adapted and transformed in digital contexts, where criminal groups may be more fluid, reputational-based and horizontally distributed than traditional hierarchies (Di Nicola, 2022).

To Victimology: The research contributes to understanding intersectional vulnerability in financial crime, demonstrating that vulnerability to fraud is multidimensional—combining economic desperation, gender-based marginalization, cognitive limitations, digital illiteracy and institutional isolation—and that perpetrators deliberately engineer

social and technological contexts to maximize exploitation (Bar-Lev, 2022; Lichtenberg et al., 2021).

To Criminology and Law: The study illustrates how legal and institutional gaps in cybercrime legislation and regulatory enforcement create enabling environments for organized financial crime, and conversely, how targeted legal reform and institutional capacity building can reduce vulnerability.

4.4. Implications for Tamil Nadu and Beyond

For Tamil Nadu, the findings indicate urgent need for:

- Specialized cybercrime investigation units equipped with digital forensic capacity at district level (Tamil Nadu Police, 2025).
- Enhanced coordination between police, RBI, UIDAI, TRAI and other regulatory bodies through integrated intelligence platforms (Government of India, 2025; Reserve Bank of India, 2025).
- Dedicated fast-track courts for cyber-financial crimes with judges trained in digital evidence and complex financial transactions (Ministry of Corporate Affairs, 2023).
- Victim support centers providing legal aid, counseling and rehabilitation to fraud victims, particularly women (Lichtenberg et al., 2021).

For India nationally, the patterns suggest similar gaps and vulnerabilities exist across multiple states, indicating that national-level legislative reform and coordination are required.

5. Recommendations for Legislative, Institutional and Policy Reform

5.1. Substantive Legislative Reform

Recommendation 1: Enactment of Comprehensive Financial Cybercrime Legislation

The Union Government should enact dedicated, comprehensive legislation—to be titled the Financial Cybercrime Prevention and Victim Protection Act, 2026—with the following key substantive provisions (Ministry of Corporate Affairs, 2023; Doon Law Mentor, 2025):

Offence Definitions:

- Mule Account Facilitation Offence: Define and criminalize the knowing misuse, operation or facilitation of others' bank accounts for layering or transferring illegal funds, with graduated penalties based on amounts and number of accounts involved.
- Identity-Based Loan Fraud Offence: Define as a specific offence the fraudulent procurement of loans using another person's identity without informed consent, with enhanced penalties when targeting vulnerable groups.
- Cyber-Enabled Financial Exploitation: Create an offence addressing systematic exploitation of digital financial systems to defraud vulnerable populations, with aggravating factors including targeting of women, elderly, economically disadvantaged individuals.
- Organized Financial Cybercrime: Establish enhanced penalties for offences perpetrated by organized groups (as defined), with specific recognition of transnational elements.

Victim Protection Provisions:

- Liability Relief for Victims: Explicitly exempt victims of identity-based loan frauds from legal liability for loans procured without their informed consent or knowledge.
- Interim Relief: Enable courts to grant interim compensation to victims during investigation and trial, recognizing ongoing economic hardship.
- Victim Compensation Fund: Establish a Central Financial Cybercrime Victim Compensation Fund (₹500 crore annually) administered by National Legal Services Authority (NALSA), providing automatic interim compensation (50% of proven loss, maximum ₹50 lakh) within 30 days of victim application, with final compensation following case resolution (Government of India, 2025).

Sentencing Framework:

- Base sentence of 5–7 years for organized financial cybercrime (as distinct from 3–5 years for non-organized offences).
- Enhanced sentencing (7–10 years) for crimes specifically targeting vulnerable populations (women, elderly, economically disadvantaged).
- International trafficking of proceeds: 10–15 years imprisonment.
- Mandatory asset forfeiture equivalent to 150% of proceeds derived (or ₹1 crore, whichever is greater).

5.2. Procedural and Investigative Reform

Recommendation 2: Specialized Financial Cybercrime Investigation Infrastructure

- Central Financial Cybercrime Investigation Bureau: Establish dedicated bureau under Ministry of Home Affairs with:
  - Staffing: 500+ specialized officers (investigators, digital forensics specialists, financial crime analysts, prosecutors) by 2027.
  - Regional Digital Forensics Labs: 5 advanced labs across major regions with ISO/IEC 27037-compliant equipment and trained personnel.
  - Training: Mandatory 6-month specialized training program in financial crime investigation, digital forensics, and organized crime analysis for all personnel.
  - Multi-Jurisdictional Authority: Explicit authority to take over investigations from state police when cases involve interstate elements, international coordination, or affect 50+ victims.
- District-Level Cyber Units: Establish dedicated cybercrime cells at each district police headquarters with minimum staffing of 10–15 officers, digital forensic equipment, and regular training (Tamil Nadu Police, 2025).

Recommendation 3: Fast-Track Adjudication Mechanisms

- Specialized Financial Cybercrime Courts: Establish dedicated courts in district headquarters with:
  - Single dedicated judge with mandatory 3-month specialized training in digital evidence, financial crime investigation and victim-sensitive proceedings.
  - Supporting staff including digital evidence managers, financial crime analysts and victim liaison officers.
  - Mandatory case completion within 18 months from charge-sheet filing.

- Virtual trial capability to facilitate victim examination without travel burdens.
- Simplified evidence procedures for bank records, digital logs and call detail records (admissible with institutional certification, without live officer testimony).
- Automatic case escalation and appellate expediting (12-month completion target for appellate decisions).

5.3. Regulatory and Institutional Reform

Recommendation 4: Enhanced Banking Sector Regulation and Oversight

- Mandatory Biometric Verification: All account opening above ₹10,000 annual transaction capacity require in-person fingerprint or iris biometric verification (Reserve Bank of India, 2025).
- Multiple Document Verification: For accounts with high-risk profiles (previous fraud complaints, multiple Aadhaar linking, occupations susceptible to mule recruitment), require minimum 3 independent identity documents plus third-party address verification.
- Enhanced Due Diligence (EDD): Accounts linked to previous fraud complaints or displaying suspicious patterns subject to automatic EDD review before fund transfers exceeding ₹50,000; delayed transaction release (24–48 hours) pending manual review.
- Real-Time Transaction Monitoring: Implementation of AI/ML-based behavioral analytics by all banks and NBFCs with assets >₹1,000 crore by December 2026, replacing rule-based threshold systems; real-time flagging of anomalous patterns (rapid multi-account transfers, velocity anomalies, structuring patterns).
- Centralized Fraud Intelligence Platform: RBI to establish platform integrating transaction data from all regulated entities, enabling pattern recognition across institutional silos and automated alert generation.
- Branch Manager Accountability: Branch managers held personally liable (in addition to bank liability) for KYC violations; implementation of periodic KYC audits with non-compliance penalties (fine, salary reduction, personnel removal authority).

Recommendation 5: Microfinance Sector Reform

- Consent Documentation Standards: Require in-person, audio-visual recorded consent for loans above ₹50,000; mandatory document delivery in local language with comprehension verification.
- Centralized Borrower Database: NABARD to establish linked database preventing multiple simultaneous loan applications to same individual across institutions; automatic fraud alerts on duplicate applications.
- Enhanced Agent Oversight: Mandatory supervision of microfinance agents with periodic audits, verification of applicant presence and identity, and agent accountability for fraud.
- Victim Protection in Loan Contracts: Explicit provision that borrowers are not liable for loans procured through fraud or without genuine consent; authority for microfinance institutions to write off fraudulently procured loans.

5.4. Digital Literacy and Community Awareness

Recommendation 6: Targeted Digital and Financial Literacy Programs

- Government Curriculum Development: Ministry of Electronics & IT to develop specialized curriculum focusing on:
  - Online banking security and fraud prevention
  - Loan documentation comprehension and contractual understanding
  - Digital payment safety and verification mechanisms
  - Recognition of fraudulent schemes and social engineering tactics
  - Consumer protection mechanisms and complaint filing procedures
- Implementation through Existing Networks: Partner with Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) to integrate financial fraud awareness into existing digital literacy training (current coverage: 6+ crore households); integrate into government primary and secondary school curricula in rural areas; disseminate through SHGs, microfinance institutions, community radio and Doordarshan.

Recommendation 7: Gender-Focused Awareness and Women Empowerment

- Digital Sakhi Program Expansion: Expand "Digital Sakhi" initiative to all rural areas of Tamil Nadu; train 1+ lakh rural women as community financial literacy educators and fraud-prevention advocates.
- SHG Integration: Partner with existing women's Self-Help Groups for in-situ fraud prevention training, enabling peer-to-peer education and collective protective mechanisms.
- Government Scheme Clarity: Launch dedicated campaigns in native languages clarifying legitimate government financial schemes, distinguishing from fraudulent imitations, and providing contact information for verification.

5.5. Victim-Centered Support and Compensation

Recommendation 8: State-Level Victim Support Centers

Each state government to establish Financial Cybercrime Victim Support Centers in district headquarters and select block headquarters with services including:

- Legal Aid: Free legal consultation, representation in compensation claims, and assistance in criminal justice participation.
- Psychological Counseling: Trauma-informed counseling for psychological impact; family mediation for intra-household relationship strain caused by victimization.
- Financial Counseling: Debt management counseling; assistance with microfinance institution negotiations for loan write-off or settlement.
- Livelihood Rehabilitation: Vocational training, microcredit linkages, and employment support for victims unable to resume prior occupations.
- Documentation Support: Assistance in filing police complaints, victim impact statements, compensation applications and accessing legal aid.

Recommendation 9: Victim Compensation Framework

- Automatic Interim Compensation: Upon victim application with basic documentation, 50% of claimed loss (maximum ₹50 lakh) disbursed within 30 days through NALSA-administered Central Financial Cybercrime Victim Compensation Fund.

- Final Compensation: 100% of verified loss following criminal case resolution or, if prosecution unsuccessful, at conclusion of investigation upon production of evidence of fraud and loss.
- Special Provisions for Loan Fraud Victims: Victims of fraudulent loan scams explicitly declared not liable for loan repayment; loans to be written off by lending institutions; compensation to cover psychological trauma, livelihood disruption and rehabilitation costs.
- Monitoring and Accountability: Dedicated Victim Rights Officer in each police station and district; NALSA-maintained centralized database tracking compensation applications, disbursements and outcomes.

6. Conclusion

The examination of financial cybercrimes in Tamil Nadu—specifically mule account fraud and fake microfinance loan scams—reveals sophisticated, organized and systematic exploitation of vulnerable populations through deliberate weaponization of digital illiteracy and regulatory gaps. Rural women, daily wage workers, and economically marginalized individuals are targeted not incidentally but as part of calculated strategy.

The evidence validates the hypothesis that current legal and institutional frameworks are inadequate. The Bharatiya Nyaya Sanhita, 2023, while more comprehensive than its predecessor, provides only general provisions addressing cheating and organized crime without specific recognition of cyber-enabled financial crime's distinctive elements—identity misuse, digital account manipulation, systemic targeting of vulnerable groups, transnational coordination.

Yet the pathways to reform are clear. Dedicated legislation, specialized law enforcement infrastructure, enhanced banking regulation, targeted digital literacy, and victim-centered compensation mechanisms can substantially reduce vulnerability and enhance justice. The recommendations offered in this study provide a comprehensive roadmap for legislative and policy reform at state and national levels.

The urgency cannot be overstated. With cumulative losses exceeding ₹52,976 crore nationally and mule account networks expanding at 83% annually, financial cybercrime represents not merely a criminal justice concern but a threat to financial stability, consumer protection, and economic justice. Tamil Nadu, as an economically advanced state with significant digital adoption, offers both a cautionary example and an opportunity for pilot reform implementation that can inform national policy.

References

Bar-Lev, E. (2022). Financial frauds' victim profiles in developing countries: A scoping review. *Frontiers in Psychology, 13*, Article 999053. https://doi.org/10.3389/fpsyg.2022.999053

Central Bureau of Investigation. (2025, June 25). *Press release: CBI conducts searches at 42 locations in Operation Chakra-V targeting mule bank accounts* [Press release]. https://cbi.gov.in/press-detail

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Deviant Behavior, 43*(5), 592–608. https://doi.org/10.1080/01639625.2020.1829139

Doon Law Mentor. (2025, March 20). *Cybercrime under Bharatiya Nyaya Sanhita: Challenges*. Retrieved from https://doonlawmentor.com/cybercrime-under-bharatiya-nyaya-sanhita-challenges/

Government of India. (2025, March 11). Government implements schemes under Nirbhaya Fund [Press release]. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2110881

Government of India. (2025, October 31). RBI advises banks to integrate DoT's Financial Fraud Risk Indicator [Press release]. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2141616

GK Today. (2026, January 4). *Why India's cyber fraud losses are surging and what the data reveals about the new crime economy*. Retrieved from https://www.gktoday.in/why-indias-cyber-fraud-losses-are-surging-and-what-the-data-reveals-about-the-new-crime-economy/

Harding, N., Button, M., Kapoor, R., & Tunley, M. (2025). Reimagining fraud theory to inform financial crime prevention. *British Journal of Criminology, 65*(3), 618–635. https://doi.org/10.1093/bjc/azae030

HyperVerge. (2025, December 16). *Bank account verification regulations: How to be compliant*. Retrieved from https://hyperverge.co/blog/bank-account-verification-regulations/

IANS. (2026, January 10). Indians lose over Rs 52,976 crore to cyber frauds over six years: Report. *IANS Live*. Retrieved from https://ianslive.in/indians-lose-over-rs-52976-crore-to-cyber-frauds-over-six-years-report--20260103154943

Indian Express. (2025, August 17). Mumbai, Delhi, Bengaluru among top 10 hotspots for mule accounts in India: Centre. Retrieved from https://indianexpress.com/article/india/mumbai-delhi-bengaluru-among-top-10-hotspots-for-mule-accounts-in-india-centre-10195337/

Lichtenberg, P. A., Campbell, L., Hall, M. H., & Gross, J. L. (2021). Examining the validity of the Financial Exploitation Vulnerability Scale (FEVS). *Innovation in Aging, 5*(Suppl 1), 874. https://doi.org/10.1093/geroni/igab046.3182

Ministry of Corporate Affairs. (2023). *Bharatiya Nyaya Sanhita, 2023: Provisions on cheating and organized crime*. Government of India. Retrieved from https://www.mca.gov.in

Moneycontrol. (2026, January 2). India's cyber scam bill crosses Rs 52,976 crore in 6 years; investment fraud is the big menace. *Moneycontrol News*. Retrieved from https://www.moneycontrol.com/news/india/india-s-cyber-scam-bill-crosses-rs-52-976-crore-in-6-years-investment-fraud-is-the-big-menace-12886935.html

Reserve Bank of India. (2025). *Master Direction on Know Your Customer (KYC)* (Updated December 2025). Retrieved from https://www.rbi.org.in

Searchinform. (2025, December 31). *Decoding the anatomy of organized cybercrime*. Retrieved from https://searchinform.com/articles/cybersecurity/cyber-threats/cybercrime/organized-cybercrime/

Tamil Nadu Police. (2025). *Cybercrime case records and FIR documentation 2024-2025*. Cybercrime Wing, Tamil Nadu Police. [Local case data and FIRs: Crime Nos. 78/25 (Karur), 79/25 (Tiruppur), 229/25 (Krishnagiri), 45/25 (Coimbatore), 129/25 (Chennai)]

Testbook. (2025, July 31). *Section 318 BNS (Bharatiya Nyaya Sanhita) - Cheating*. Retrieved from https://testbook.com/judiciary-notes/section-318-bns

The News Minute. (2026, January 5). Cyber fraud losses in TN's Coimbatore cross Rs 87 crore in 2025, recovery below 10 pc. Retrieved from https://www.thenewsminute.com/tamil-nadu/cyber-fraud-losses-in-tns-coimbatore-cross-rs-87-crore-in-2025-recovery-below-10-pc

Times of India. (2026, January 5). Coimbatore residents lost Rs 87.16 crore to cyber fraudsters in 2025: Police. Retrieved from https://timesofindia.indiatimes.com/city/coimbatore/coimbatore-residents-lost-rs-87-16-crore-to-cyber-fraudsters-in-2025-police/articleshow/117012479.cms

Upstox. (2025, June 25). Over 8.5 lakh mule accounts in 700 bank branches used by cyber criminals: CBI. *Upstox News*. Retrieved from https://upstox.com/news/business-news/latest-updates/over-8-5-lakh-mule-accounts-in-700-bank-branches-used-by-cyber-criminals-cbi/

Zigram Tech. (2025, September 24). *Understanding mule accounts in tier 1 and tier 2 cities in India*. Retrieved from https://www.zigram.tech/article/mule-accounts-tier-1-tier-2-cities-india/