VOLUME 7 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ANATOMY OF INSTANT LOAN SCAMS ON MESSAGING PLATFORMS TACTICS, VICTIM VULNERABILITY AND COUNTER MEASURES

- T. Xavier Devasahayam[1]

Abstract: -

The rapid expansion of digital communication technologies has transformed the lending ecosystem by enabling instant access to financial services through messaging platforms such as WhatsApp, Telegram, Facebook Messenger, Instagram, and Signal. While these platforms facilitate convenience and financial inclusion, they have simultaneously become fertile ground for fraudulent loan operations. Instant loan scams exploit financial distress, information asymmetry, digital trust, and technological vulnerabilities to deceive potential borrowers. Victims are frequently promised unsecured loans with minimal documentation, rapid approval processes, and attractive interest rates. Once engagement begins, fraudsters employ a combination of social engineering, psychological manipulation, impersonation, identity theft, advance-fee fraud, and data extortion mechanisms.

This paper examines the anatomy of instant loan scams on messaging platforms by analyzing scam tactics, victim vulnerabilities, psychological triggers, technological enablers, and existing countermeasures. The study synthesizes findings from cybersecurity literature, financial fraud research, and digital

[1] Advocate at Madurai Bench of Madras High Court

© 2026 International Journal of Advanced Legal Research

criminology. It argues that loan scams thrive at the intersection of economic need and digital trust. The research identifies common scam stages including targeting, engagement, verification deception, monetary extraction, and victim silencing. It further explores demographic, socioeconomic, and behavioral factors contributing to victim susceptibility. Finally, the paper proposes a multidimensional framework involving regulatory intervention, platform accountability, consumer awareness, technological safeguards, and international cooperation. The findings contribute to broader discussions surrounding financial cybercrime and highlight the urgent need for an integrated response to combat loan fraud in digital spaces.

Keywords: -Instant Loan Scams, Messaging Platforms, Cybercrime, Digital Fraud, Financial Technology, Consumer Protection, Victimization, Social Engineering

1. Introduction

Digital financial services have revolutionized the accessibility of credit for millions of individuals worldwide. The emergence of financial technology (FinTech) has enabled consumers to obtain loans with unprecedented speed and convenience. Parallel to legitimate innovation, however, cybercriminals have leveraged digital platforms to execute deceptive financial schemes targeting vulnerable populations.

Messaging applications have become particularly attractive channels for fraudulent activity because they provide direct, low-cost communication with large groups of potential victims. Fraudsters can establish apparent legitimacy through professional-looking profiles, forged documents, testimonials, and automated

© 2026 International Journal of Advanced Legal Research

communication tools. The anonymity afforded by messaging platforms further complicates accountability and enforcement.

Digital credit has expanded rapidly across emerging economies. Smartphone penetration, instant payment rails, and alternative-data underwriting have let lenders reach borrowers who were previously excluded from formal finance. That expansion has been accompanied by a parallel market of fraudulent and predatory actors who imitate legitimate lenders. Some operate as outright fake lenders that never disburse a loan. Others are abusive lenders that disburse small sums and then extract far more through harassment. Both rely heavily on messaging platforms, which offer them near-zero marketing cost, end-to-end encrypted private channels, easy account replacement, and a conversational setting that feels personal and trustworthy.

In India the problem drew sustained policy attention after reports of abusive loan applications and recovery agents,[2] which prompted the Reserve Bank of India (RBI) to convene a working group on digital lending and later issue binding guidelines.[3] Law enforcement agencies have also reported operations against networks of such apps, many with cross-border links.[4] Similar patterns have been documented in Kenya, Nigeria, Indonesia, and the Philippines, which suggests a transnational scam model rather than a local anomaly.

Instant loan scams represent one of the fastest-growing forms of digital financial fraud. These scams typically promise immediate loan approval without

[2]Reserve Bank of India, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (November 2021)
[3]Reserve Bank of India, *Guidelines on Digital Lending* (September 2, 2022)
[4]Enforcement actions against loan-app networks and associated payment-gateway accounts have been publicly reported by state cyber police units and the Enforcement Directorate in 2022–2023. Cite the specific press releases or news reports you rely on, with dates

© 2026 International Journal of Advanced Legal Research

credit checks or extensive documentation. Individuals experiencing financial distress are especially susceptible to such offers, making them prime targets for exploitation.

This paper investigates how instant loan scams operate on messaging platforms and why they continue to succeed despite increasing digital awareness campaigns. By examining the tactics employed by fraudsters, the vulnerabilities of victims, and the effectiveness of current countermeasures, the study provides a comprehensive understanding of this emerging cybercrime phenomenon.

An **instant-loan scam** here means any scheme in which a person or network uses an offer of fast, low-documentation credit, communicated or consummated through a messaging platform, to obtain money, personal data, or leverage over the borrower by deception or coercion. Two archetypes are distinguished:

- **Advance-fee (phantom loan) fraud** No loan is ever disbursed. Victims pay "processing," "insurance," "GST," or "verification" fees and receive nothing.
- **Predatory or coercive lending fraud** A small loan, often with undisclosed charges and a very short tenor, is disbursed. The lender then recovers far more than is owed by threatening the borrower and the borrower's contacts using data taken from the phone.

Hybrids exist, and the boundary between "scam" and "illegal lending" is a legal question that varies by jurisdiction. The paper uses "scam" where deception about identity, terms, or existence of the loan is material.

2. Evolution of Instant Loan Scams

© 2026 International Journal of Advanced Legal Research

Traditional loan fraud historically relied on physical interactions, newspaper advertisements, or telephone communication. Digital transformation has significantly changed these practices.

Modern fraudsters utilize messaging platforms because they offer:

1. Instant communication
2. Multimedia capabilities
3. Large audience reaches
4. Limited identity verification
5. End-to-end encryption in some cases

The rise of digital payment systems has further facilitated these scams. Criminals can receive payments quickly and transfer funds across jurisdictions, reducing recovery possibilities.

Fraud operations have also become increasingly professionalized. Many scam groups operate in organized structures involving recruiters, scriptwriters, account administrators, data brokers, and money mules.

As a result, instant loan scams now resemble sophisticated criminal enterprises rather than isolated opportunistic offenses.

3. Theoretical Framework

3.1 Routine activity theory

Routine activity theory holds that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge in space and time.[5] Messaging platforms alter each element. Offenders gain reach and anonymity.

[5]Lawrence E. Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608

© 2026 International Journal of Advanced Legal Research

Targets are findable through leaked or purchased contact lists. Guardianship is thin because private chats are not moderated in the way public posts are, and because the "place" of the crime is a one-to-one conversation that bystanders cannot observe. The theory is therefore a useful organizing frame for the countermeasures in Section 7, since each countermeasure raises guardianship or reduces target suitability.

3.2 Persuasion and scam psychology

Cialdini's principles of influence (authority, scarcity, social proof, reciprocity, commitment, and liking) have been widely applied to fraud.[6] Whitty extended this into a model of scammer persuasion that stresses staged escalation and the victim's gradual loss of critical judgment.[7]Stajano and Wilson identified recurring "principles" that scammers exploit, including distraction, social compliance, herd behavior, dishonesty, kindness, need and greed, and time pressure.[8] The Office of Fair Trading's study of mass-marketed scams found that victims often act on rational-seeming but flawed reasoning triggered by emotional arousal, not carelessness alone.[9] Button and colleagues' interviews with online fraud victims likewise showed that victims frequently knew the general warning signs yet failed to apply them in the moment.[10]

3.3 Scarcity and decision-making under financial stress

[6]Robert B. Cialdini, *Influence: The Psychology of Persuasion*, rev. ed. (New York: Harper Business, 2007)
[7]Monica T. Whitty, "The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam," *British Journal of Criminology* 53, no. 4 (2013): 665–684
[8]Frank Stajano and Paul Wilson, "Understanding Scam Victims: Seven Principles for Systems Security," *Communications of the ACM* 54, no. 3 (2011): 70–75
[9]Stephen E. G. Lea, Peter Fischer, and Kath M. Evans, *The Psychology of Scams: Provoking and Committing Errors of Judgement*, Office of Fair Trading Research Paper (2009)
[10]Mark Button, Carol Nicholls, Jeremy Kerr, and Rachael Owen, "Online Frauds: Learning from Victims Why They Fall for These Scams," *Australian & New Zealand Journal of Criminology* 47, no. 3 (2014): 391–408

© 2026 International Journal of Advanced Legal Research

Mullainathan and Shafir argue that scarcity, including scarcity of money and time, narrows cognitive bandwidth and induces "tunneling," in which immediate needs crowd out longer-term evaluation.[11] A borrower facing a medical bill or an eviction notice is therefore not only more likely to seek credit but also less able to scrutinize a suspicious offer. Prospect theory's observation that people become risk-seeking when facing certain losses is also relevant: a borrower who has already paid one "fee" may pay another to avoid the loss of the first.[12]

3.4 Synthesis

The framework combines a situational lens (routine activity) with a psychological one (persuasion and scarcity). The situational lens explains where and why scams are concentrated on messaging platforms. The psychological lens explains why exposure converts into victimization. Neither alone accounts for the ecosystem, which is why both are used in the stage analysis below.

4. The Anatomy of an Instant-Loan Scam

The scam is best understood as a sequence of stages. Not every scheme includes all stages, but the ordering is consistent across reported cases.

4.1 Stage 1: Target acquisition and lure

Sourcing targets. Scammers obtain phone numbers through data breaches, scraped or sold lead lists, random-number dialing, and referral chains in which an earlier victim's contacts are harvested. Telephone numbers are enough to begin, because messaging platforms let anyone contact any registered number.

[11]Sendhil Mullainathan and EldarShafir, *Scarcity: Why Having Too Little Means So Much* (New York: Times Books, 2013)

[12]Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47, no. 2 (1979): 263–291

© 2026 International Journal of Advanced Legal Research

The lure. Contact arrives as an unsolicited message, a group invitation, an advertisement that redirects to a chat, or an SMS containing a link to a chat handle. Typical content includes pre-approved limits, "zero documentation," "instant disbursal in five minutes," and "no credit score needed." The lure is calibrated to the underserved borrower: low-income, thin-file, or credit-rejected.

Identity borrowing. Scammers commonly impersonate recognizable lenders, banks, or even regulators. They use logos, forged registration numbers, and fake certificates. A message may cite a real regulated entity's name while directing the victim to a different payment account. The impersonation exploits the authority heuristic described by Cialdini.

4.2 Stage 2: Rapport and credibility building

Once a victim replies, the conversation moves quickly to a "loan officer" persona. Typical features include:

- A professional-looking profile picture and business-style display name.
- Scripted but personalized language, often in the victim's regional language.
- Fabricated social proof: screenshots of "approved" loans, testimonials, or a group chat populated by accomplices posting success stories.
- A formal process that mimics real lending: application forms, ID uploads, selfie verification, and "loan agreement" PDFs.

This stage serves two purposes. It builds trust, and it captures sensitive data (identity documents, bank details, selfies) that can later be used for identity fraud or as leverage. The documentary process creates a sense of legitimacy and a

© 2026 International Journal of Advanced Legal Research

commitment trap: having invested effort in the application, the victim is psychologically predisposed to see it through.

4.3 Stage 3: Fee extraction (advance-fee variant)

At the point where the loan would be disbursed, a problem is introduced. The victim is told that a fee must be paid first. Reported justifications include processing charges, refundable security deposits, insurance, tax or GST, "credit score unlocking," wrong bank details requiring a "correction" payment, or AML clearance. Payments are requested to personal UPI IDs, wallet accounts, or mule bank accounts, often in small tranches.

The scheme escalates. Each payment is framed as the last, and each new obstacle is explained as a technical or regulatory hitch. This exploits sunk-cost reasoning and loss aversion. Deadlines such as "offer expires in 30 minutes" reduce deliberation. Where the victim hesitates, the scammer may threaten to cancel the loan or to report the victim for "non-cooperation."

4.4 Stage 4: Data and device capture (predatory variant)

In the abusive-app variant, the victim is directed to install an application through a link shared on the messaging platform, frequently outside official app stores or through short-lived store listings. Installation requests extensive permissions, including contacts, photos, SMS, call logs, and sometimes storage and location. The permissions are unrelated to credit assessment but are essential to the later coercion. Platform operators have since tightened policies on personal-loan apps, partly in response to such misuse.[13]

[13]Google Play Developer Policy Center, policies on personal loan apps (introduced and revised 2020–2022). Cite the policy version and access date

© 2026 International Journal of Advanced Legal Research

4.5 Stage 5: Disbursal on abusive terms and coercive recovery

A small amount is disbursed, often substantially less than the sanctioned figure because of deducted "processing fees" and charges. Repayment is demanded within days, with effective annualized costs that can reach extreme levels. When the borrower pays late or disputes the amount, recovery agents begin a pattern of harassment:

- Abusive and threatening messages and calls.
- Messages sent to the borrower's contacts, including family, employers, and friends, announcing that the borrower is a "fraudster" or "defaulter."
- Morphed or sexualized images of the borrower circulated to contacts.
- Threats of police action, legal notices that appear official, or physical harm.

Reports have linked such harassment to severe distress and, in documented cases, to suicides, which is part of what prompted regulatory scrutiny. The coercion is effective precisely because the data was obtained through the permissions granted at installation. Shame, rather than debt, becomes the primary lever.

4.6 Stage 6: Cash-out, laundering, and churn

Proceeds move through layered accounts. Mule accounts, often opened with stolen or rented identities, receive and forward funds. Payment aggregator accounts, prepaid wallets, and crypto conversion are used to obscure the trail. Enforcement agencies in India have reported actions involving payment gateway accounts linked to loan-app operators. Infrastructure is disposable. Phone numbers, messaging accounts, app listings, and bank accounts are discarded and replaced when reported, so takedown of a single node rarely disrupts the network.

© 2026 International Journal of Advanced Legal Research

4.7 Summary table of stages

Stage	Offender objective	Key persuasion lever	Primary victim harm
Lure	Reach and attract	Greed/need, authority	Exposure
Rapport	Trust and data	Liking, social proof, commitment	Data loss
Fee extraction	Money	Time pressure, sunk cost	Direct financial loss
Data capture	Leverage	Compliance, permissions habituation	Privacy loss
Coercive recovery	Inflated repayment	Fear, shame, social exposure	Financial and psychological harm
Cash-out	Laundering	n/a	Recovery difficulty

5. Tactics: A Taxonomy of Persuasion and Deception

5.1 Authority and impersonation

Scammers invoke regulators, banks, and government schemes. They may cite plausible but unverifiable license numbers, or claim to be partners of known institutions. Because ordinary borrowers rarely know how to check a lender's registration, such claims function as credentials. Verification is difficult in practice,

© 2026 International Journal of Advanced Legal Research

which is one reason regulators have moved toward public registries of permitted lending apps and regulated entities.[14]

5.2 Urgency and artificial scarcity

Limited-time offers, quota claims ("only 5 loans left today"), and countdowns compress decision time. Because stress already narrows cognitive bandwidth,urgency compounds an existing vulnerability instead of merely adding to it.

5.3 Social proof and the fake community

Group chats seeded with accomplices, "customer" testimonials, and screenshots of disbursed funds create a herd effect. Stajano and Wilson identify herd behavior as a core exploit: people infer safety from the apparent actions of others.Because such groups are private, the victim cannot easily see that members share creation dates or posting patterns.

5.4 Reciprocity and incremental commitment

Small initial favors, such as a "free eligibility check" or quick replies, are followed by escalating asks. Each completed step (uploading a document, paying a small fee) increases commitment. The victim's self-image as a rational person who has done the right steps makes quitting costly.

5.5 Fear, shame, and coercion

In the abusive-lending model, the dominant tactic shifts from inducement to threat. Public exposure of purported debt, contact harassment, and image manipulation exploit social stigma around indebtedness. This tactic is notable

[14]Ministry of Finance, Government of India, draft *Banning of Unregulated Lending Activities Bill* (released for public consultation, 2024)

© 2026 International Journal of Advanced Legal Research

because it can succeed against borrowers who knew the terms were unfair. The victim is trapped by leverage, not by deception alone.

5.6 Technical camouflage

Techniques include fake app listings that mimic legitimate lender names, links that redirect through multiple domains, cloned websites, and spoofed or "virtual" numbers. Phishing pages harvest net-banking credentials or card data under the guise of "verification." Some messages instruct victims to enable screen sharing or remote access tools, extending the attack from advance-fee fraud to account takeover.

5.7 Exploitation of platform affordances

Messaging platforms provide features that scam operators exploit: bulk-forwarding of messages, group invites that bypass sender screening, business account badges that confer a veneer of authenticity, disappearing messages that erase evidence, and end-to-end encryption that prevents server-side content scanning. These features serve legitimate privacy and usability goals, which is why the countermeasure debate is genuinely difficult.

6. Victim Vulnerability

Vulnerability to financial scams is not reducible to a single demographic. Evidence from victimology research stresses that anyone can be defrauded and that vulnerability is often situational. The paper distinguishes four clusters.

6.1 Economic precarity and credit exclusion

Households with irregular income, thin credit files, or rejected formal credit applications are natural targets. Their need is real and often urgent, and their

© 2026 International Journal of Advanced Legal Research

alternatives are limited. Informal moneylenders may be expensive or socially visible, so a private chat offering anonymous credit can seem attractive. Scarcity-induced tunneling reduces the cognitive resources available for verification.

6.2 Digital and financial literacy gaps

Many first-time smartphone users lack a mental model of app permissions, URL structure, or the distinction between regulated and unregulated lenders. Language matters too. Warnings and consumer-protection information are less accessible to people who do not read the dominant language of official communication. Permission prompts are routinely accepted by habit, which is precisely the behavior the abusive-app model relies on.

6.3 Emotional state and life events

Medical emergencies, job loss, debt spirals, and family crises raise both the demand for fast credit and susceptibility to emotional manipulation. Scammers often target such windows, including by buying lead lists of people who have recently searched for loans or interacted with loan advertisements. Repeat victimization is a recognized phenomenon: previous victims may be re-contacted by "recovery" scammers promising to retrieve lost money for a fee.

6.4 Social and structural factors

Stigma and underreporting. Shame about debt and about having been tricked suppresses reporting, which weakens enforcement data and allows operators to continue.Gender and safety. Image morphing and sexualized threats make women particularly exposed to coercion in the predatory model.Because harassment reaches a victim's contacts, vulnerability is socially distributed. A single compromised phone exposes an entire network and can seed new targets.

© 2026 International Journal of Advanced Legal Research

Institutional distrust. Victims who expect to be disbelieved, or who fear their own legal exposure (for example, for having borrowed from an unregulated app), are less likely to approach police or banks.

6.5 Implications

Three points follow. First, awareness campaigns alone are insufficient, because the literature shows that knowing about scams does not reliably prevent victimization under stress and time pressure. Second, the best interventions reduce the need for victims to make perfect judgments by adding friction, defaults, and accessible verification. Third, support for victims, including psychological and legal help, is a prevention measure as well as a remedy, because it encourages reporting and reduces repeat victimization.

7. Countermeasures

7.1 Platform-level measures

Account-level detection and enforcement. Messaging providers can detect behavioral signals of bulk scam operations, such as mass messaging from new accounts, rapid group creation, and high report rates, without needing to read message content. Under India's intermediary rules, large platforms are required to publish periodic compliance reports describing actions against abusive accounts, which provides at least a minimal accountability channel.[15]Friction at the point of risk. Warnings when an unknown number sends a link, labels that identify accounts as recently created or as outside the user's contacts, and forwarding limits reduce impulsive engagement. This reflects the "nudge" logic of designing choice

[15]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(1)(d) (monthly compliance reporting by significant social media intermediaries)

© 2026 International Journal of Advanced Legal Research

environments to counter predictable biases.[16] Friction should be targeted, since blanket warnings produce habituation.Verified business identity. Business verification badges are useful only if verification is rigorous. A weak badge is worse than none because it lends borrowed authority to scammers. Platforms should link verification to regulatory registries where lenders must be registered.App-store and distribution controls. Official app marketplaces can require proof of regulatory authorization for lending apps, restrict sensitive permissions, and remove violators. Such policies have been tightened in recent years, though enforcement lags and sideloaded installation through links shared in chats remains a gap. End-to-end encryption prevents content scanning by design. Proposals that would require traceability or weaken encryption are contested on privacy and security grounds. A more defensible approach emphasizes metadata signals, client-side warnings, and user reporting tools. The paper takes the position that scam mitigation should not be used to justify a general weakening of encryption, and that effective alternatives exist.

7.2 Financial-infrastructure measures

Mule account controls. Because every scheme ends in a cash-out, banks and payment providers are strategic chokepoints. Measures include stronger onboarding checks, transaction monitoring for rapid in-and-out flows, velocity limits on new accounts, and information sharing across institutions about flagged accounts.Confirmation prompts for first-time payees, name-matching displays, and short cooling-off delays for high-risk transaction patterns can interrupt scam payments. Evidence from behavioral research suggests that small delays help most when the victim is acting under artificial urgency.Enforcement actions have

[16]Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (New Haven: Yale University Press, 2008)

© 2026 International Journal of Advanced Legal Research

targeted payment intermediaries accused of enabling loan-app operators. Clear due-diligence obligations on merchant onboarding, with penalties for lax controls, shift responsibility to the institutions best placed to detect abuse.

The speed of response is decisive. India's national cybercrime reporting portal and helpline (1930) were designed to let victims report quickly so that funds can be frozen before they move on.[17] Wider and faster bank participation, and clearer rules on restitution, would increase recovery rates.

7.3 Regulatory and legal measures

The RBI's working group report and the 2022 digital lending guidelines established principles including disclosure of the lending service provider's role, a key fact statement, direct disbursal into and repayment from borrower bank accounts, restrictions on data collection, and a cooling-off period. Subsequent consolidated directions on digital lending continue this approach verify the current status and title of the 2025 directions before citing.[18] A government draft bill proposed in 2024 would criminalize unregulated lending activity and establish a registry, although the paper's author should verify its current legislative status.

Relevant provisions include the Information Technology Act's sections on identity theft and cheating by personation using computer resources,[19] and the Bharatiya Nyaya Sanhita's provisions on cheating, extortion, and criminal intimidation.[20] Prosecutors face evidentiary challenges, since messages are ephemeral and operators are often abroad.

[17]Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), National Cyber Crime Reporting Portal and helpline 1930
[18]Reserve Bank of India, *Digital Lending Directions, 2025*
[19]Information Technology Act, 2000, ss. 66C and 66D
[20]Bharatiya Nyaya Sanhita, 2023, provisions on cheating, extortion, and criminal intimidation

© 2026 International Journal of Advanced Legal Research

The Digital Personal Data Protection Act, 2023 introduces obligations on data fiduciaries concerning consent and purpose limitation, which in principle constrain the over-collection of contacts and photographs by lending apps.[21] Its effectiveness will depend on rules, enforcement capacity, and public awareness.

Many networks have overseas components. Mutual legal assistance is slow relative to the speed at which infrastructure is churned. Intelligence sharing, joint operations, and sanctions on facilitators are therefore necessary complements to domestic action.

7.4 Telecom and ecosystem measures

Telecom regulators have introduced mechanisms for citizens to report suspected fraudulent communications and to check and block numbers linked to their identity.[22] SIM-issuance controls, detection of bulk-registered numbers, and action against spoofed calling lines target the upstream resource scammers depend on. Because phone numbers are the identity layer for messaging platforms, telecom controls have an outsized effect on offender capacity.

7.5 User-level and community measures

Verification habits. A short, memorable checklist is more effective than extensive literacy training.

For example:

(1) Is the lender on the regulator's published list?

(2) Does the lender ask for money before disbursing?

[21]Digital Personal Data Protection Act, 2023

[22]Department of Telecommunications, Government of India, Sanchar Saathi portal and the Chakshu facility for reporting suspected fraudulent communication

© 2026 International Journal of Advanced Legal Research

(3) Does the app request permissions unrelated to lending?

(4) Am I being rushed?

A "no" to the first or a "yes" to any of the others should halt the process.

Self-help groups, employers, community organizations, and local-language media are trusted channels. Interventions that use them reach populations that formal advertising does not.

Accessible counselling, legal aid, and non-judgmental reporting channels reduce the stigma that sustains the coercive model. A victim who knows that harassment of their contacts is illegal and reportable is less susceptible to that tactic.

7.6 An integrated model: friction and accountability

Friction consists of measures that slow or interrupt the victim's path at critical moments: warnings, payee checks, permission prompts, and cooling-off periods. Accountability consists of measures that raise the cost to offenders and facilitators: verified identity, mule account liability, aggregator due diligence, and prosecution. Friction without accountability merely displaces scammers to the next channel. Accountability without friction acts too late for victims. Policy should therefore be assessed on whether it supplies both.

8. Conclusion

Instant-loan scams on messaging platforms are best understood as an organized, staged enterprise that converts financial need into profit through manufactured trust, urgency, and fear. Their effectiveness comes from a fit between

© 2026 International Journal of Advanced Legal Research

offender tactics and the situational vulnerabilities of credit-excluded, time-pressed borrowers, within a communication environment that offers reach, privacy, and little guardianship. Awareness alone is a weak defense, because victims often know the warnings but cannot apply them under stress.

A durable response must therefore operate on multiple layers. Platforms can introduce targeted friction and verified identity. Financial institutions can choke off cash-out routes. Regulators and prosecutors can raise the cost of offending and clarify liability for facilitators. Telecom authorities can restrict the supply of numbers. Communities and support services can reduce the shame that sustains coercive recovery. Underlying all of this, expanding access to affordable regulated credit addresses the demand that scammers exploit. The friction-and-accountability model offered here is a starting point for empirical testing, and its propositions should be evaluated with better data than currently exists.

© 2026 International Journal of Advanced Legal Research