Review of International Geographical Education | RIGEO | 2020

RIGEO

ISSN: 2146 - 0353

Review of International GEOGRAPHICAL EDUCATION

www.rigeo.org

Cyber Enabled Financial Fraud in the Digital Payments Era: A Qualitative Content Analysis

Ms. Prabha A
Ph.D Scholar, Reg. No. 18214012042057, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, India

Prof. Dr. Beulah Shekhar
Adjunct Professor, Parul Institute of Liberal Arts, Parul University, India

ABSTRACT

Cyber enabled financial fraud has expanded alongside the mainstreaming of digital payments, online banking, and platform mediated communication, producing high volume victimisation that often relies on deception and social engineering rather than advanced technical intrusion. While policy and institutional responses increasingly emphasise rapid reporting and coordinated action, there is limited systematic research on how authoritative texts frame harm, victimhood, responsibility, and remedy. This study applies qualitative content analysis to a purposive corpus of 20 governance and institutional response documents drawn primarily from India, including regulatory instruments, incident reporting directives, policing advisories, and citizen facing reporting guidance, supplemented by selected global benchmark reports for contextual comparison. Using a directed coding frame with inductive refinement, the analysis examines problem definitions, harm framing, victim positioning, reporting pathway construction, institutional responsibility allocation, coordination expectations, and remedy narratives.

Findings identify six dominant themes. First, cyber financial fraud is constructed as a scalable deception ecosystem, with impersonation and persuasion central to offence execution. Second, speed is framed as the primary determinant of outcome, creating a governance logic of a “golden hour” for reporting and intervention. Third, reporting pathways are presented as multi entry but not consistently articulated as a coherent end to end victim journey. Fourth, although responsibilities are distributed across police, banks, payment systems, and cyber incident authorities, public facing messaging often recentres individual vigilance and compliance. Fifth, victim protection is operationalised mainly through liability limitation and compensation logic, reflecting a consumer protection and trust preservation orientation. Sixth, psychosocial harms, stigma, and secondary victimisation risks are weakly articulated relative to procedural and compliance priorities. The study concludes that strengthening journey clarity, low friction evidence expectations, empathetic communication standards, accountable timelines, and rapid coordination can improve timely reporting, reduce underreporting, and support recovery that extends beyond financial remedy.

Keywords: *cybercrime, cyber enabled financial fraud, digital payments, content analysis, governance texts, victimology, reporting, institutional response*

INTRODUCTION

Cyber enabled financial fraud has become one of the most visible forms of contemporary cybercrime because it thrives in the everyday infrastructure of digital payments, online banking, and platform based communication. Unlike intrusion led cyber offences that depend on complex technical exploitation, many high frequency frauds rely on deception, impersonation, and coercive persuasion that can be executed at scale with minimal technical effort. Complaint based evidence from the FBI Internet Crime Complaint Center consistently shows that phishing and spoofing dominate complaint volumes, while investment related fraud produces extremely high aggregate losses, and older adults face disproportionate harm (Federal Bureau of Investigation, Internet Crime Complaint Center, 2024). This pattern supports the view that cyber enabled financial fraud is best understood as an interactional crime where offenders engineer urgency, authority cues, and trust signals to compress the victim's decision window, rather than as a problem of technology alone (United Nations Office on Drugs and Crime, 2013).

In India, rapid adoption of instant payment systems and digital banking has expanded the opportunity structure for fraud while also compressing the time available for containment and recovery. Governance responses increasingly highlight timely reporting and coordinated action as essential, because once funds move through layered accounts, recovery becomes significantly more difficult. Key institutional actors shape this ecosystem through public reporting architecture, policing workflows, and regulatory protection frameworks. For example, the Reserve Bank of India has issued customer protection rules that limit customer liability in unauthorised electronic banking transactions under specified conditions, creating a formal remedy and responsibility allocation logic (Reserve Bank of India, 2017). At the same time, cyber incident governance norms, including those issued by CERT-In, embed rapid reporting requirements for specified entities, signalling that speed is treated as a core governance variable in cyber risk containment (Indian Computer Emergency Response Team, 2022).

Despite this growing policy attention, two gaps remain significant in the scholarly and applied literature. First, much cyber fraud work focuses on typologies, prevalence, and technical countermeasures, while giving less systematic attention to how authoritative texts define harm, position victims, and allocate institutional responsibility. Second, while underreporting is widely recognised, it is often treated as a citizen behaviour issue rather than as a governance communication and system design issue shaped by stigma, blame expectations, fragmented reporting routes, and perceived futility (Blakeborough & Gira Correia, 2018; Cross et al., 2016). Victimology research shows that fraud can generate lasting psychological and social harms including distress, shame, self blame, sleep disruption, and withdrawal, which may be intensified when institutional processes are unclear or experienced as blame oriented (Button et al., 2014; Cross et al., 2016). When governance texts prioritise procedural compliance without equally emphasising victim legitimacy, predictable timelines, and supportive communication, they may unintentionally raise the threshold for reporting and cooperation.

To address these gaps, this study conducts a qualitative content analysis of authoritative governance and institutional response texts on cyber enabled financial fraud. The study examines how fraud is framed, which harms are prioritised, how victims and offenders are represented, how reporting urgency is constructed, and how responsibility and coordination are distributed across institutions. By treating policy and operational texts as instruments of governance rather than neutral information, the analysis identifies dominant frames, recurring silences, and points where messaging and workflow design may shape reporting behaviour and recovery expectations (Hsieh & Shannon, 2005; Krippendorff, 2019; Schreier, 2012). The paper contributes a victim centred governance reading of cyber fraud, highlighting how the architecture of reporting and response is not only technical and legal, but also communicative and procedural, with direct implications for trust, underreporting, and victim recovery.

Cybercrime and the rise of cyber enabled financial fraud

Cybercrime has expanded alongside the rapid normalisation of digital payments, online banking, and platform mediated communication, producing a high frequency environment for financial frauds that rely more on deception than on advanced technical intrusion. Contemporary cyber enabled fraud increasingly centres on social engineering, where offenders manipulate attention, trust, and urgency to induce victims to authorise transfers or disclose credentials, rather than relying solely on technical compromise (United Nations Office on Drugs and Crime, 2013). Large scale complaint based evidence in the United States indicates that phishing and spoofing continue to dominate the volume of cybercrime complaints, while investment related fraud generates exceptionally high aggregate losses, and older adults face disproportionate harm (Federal Bureau of Investigation, Internet Crime Complaint Center, 2024).

This pattern matters for theory and policy because it reframes cyber financial fraud as an interactional crime. It is often an offence of persuasion, credibility signalling, and situational pressure, rather than a purely technical attack. Within this framing, the victim is not simply a careless user. The victim is a decision maker placed under engineered urgency, asymmetric information, and perceived authority cues that compress deliberation time and increase compliance likelihood (United Nations Office on Drugs and Crime, 2013).

In India, official crime statistics are compiled and published annually by the National Crime Records Bureau in its Crime in India series. A parliamentary response from the Ministry of Home Affairs notes that the latest published Crime in India report is for the year 2023, while also clarifying that victim reporting percentages for online fraud are not maintained by the NCRB (Ministry of Home Affairs, 2025).

Understanding harms beyond financial loss

A growing victimology literature demonstrates that fraud and cyber fraud are not victimless offences. Research on fraud victims consistently documents psychological and social harms, including distress, anxiety, anger, self blame, shame, sleep disruption, and withdrawal, with effects that can persist beyond the financial incident, particularly when outcomes remain uncertain or recovery processes are slow (Button et al., 2014). These harms often interact with identity and reputation concerns, because fraud victimisation can trigger embarrassment and fear of judgement, which in turn shapes disclosure and help seeking (Button et al., 2014).

In the context of online fraud, qualitative evidence from Australia shows that victims frequently describe shame and embarrassment alongside distress and rumination, and they emphasise support needs that extend beyond transactional recovery, including clear guidance and humane responses (Cross et al., 2016). This is consistent with UK evidence synthesis indicating that non reporting is commonly linked to shame, embarrassment, fear of not being believed, and self attribution of blame, alongside perceptions that reporting will not produce meaningful outcomes (Blakeborough & Gira Correia, 2018).

These findings are important because cyber financial fraud often concentrates victimisation within a narrow decision window. Offenders frequently exploit authority cues, urgency cues, and coercive persuasion. This reduces the cognitive space for verification and increases the likelihood of compliance, which challenges narratives that attribute cyber fraud primarily to carelessness or ignorance (United Nations Office on Drugs and Crime, 2013).

Underreporting and the reporting decision

Underreporting is a consistent feature of fraud and cyber enabled crimes, shaped by emotional barriers and perceived futility. Evidence synthesis in the UK highlights that reporting decisions reflect both personal barriers, such as shame, embarrassment, and fear of disbelief, and practical calculations about time, effort, and anticipated benefit (Blakeborough & Gira Correia, 2018). In cyber fraud contexts, victims may also fear blame oriented responses or feel they will be treated as responsible for their own loss, which further elevates the psychological threshold for reporting (Cross et al., 2016; Blakeborough & Gira Correia, 2018).

Complaint based reporting systems also implicitly acknowledge undercounting, since recorded complaints represent reporting behaviour rather than true incidence. Even so, large scale complaint data remains valuable for identifying dominant modus operandi and harm concentrations across groups. For example, the Internet Crime Complaint Center report documents very high complaint volumes and losses, with older adults experiencing especially high losses, reinforcing the need to treat reporting pathways and rapid response as core harm reduction mechanisms (Federal Bureau of Investigation, Internet Crime Complaint Center, 2024).

From a systems perspective, the reporting decision is not only an individual psychological choice. It is also a system design outcome. When reporting pathways are fragmented, guidance is inconsistent, or victims anticipate judgement, the likelihood of reporting declines. Conversely, when institutions communicate clear first steps, provide quick acknowledgement, and offer predictable timelines, reporting becomes more likely and time sensitive interventions, such as fund holds and tracing, become more feasible (Cross et al., 2016; United Nations Office on Drugs and Crime, 2013).

Institutional response and consumer protection framing

Institutional response to cyber enabled financial fraud spans police, regulators, banks, payment systems, and digital platforms. In consumer banking, one key policy lever is liability allocation, coupled with timeliness of reporting. The Reserve Bank of India issued the Customer Protection circular on limiting liability of customers in unauthorised electronic banking transactions, outlining conditions under which customer liability may be limited, and emphasising that banks must take immediate steps after being notified to prevent further unauthorised activity (Reserve Bank of India, 2017).

Recent policy attention also signals a continued shift toward treating cyber fraud as a consumer protection issue, not only a law enforcement issue. Reuters reporting in February 2026 described a proposed framework to compensate customers for small value digital payment frauds, indicating a governance emphasis on remedy and trust in digital payment systems

(Reuters, 2026). For the present study, the relevance is narrative and institutional framing. It shows how policy texts define harm, responsibility, and what counts as an adequate remedy (Reuters, 2026).

Cyber incident governance and mandatory reporting norms

Governance narratives also include mandatory cyber incident reporting requirements for service providers and intermediaries. CERT In directions issued under the Information Technology Act framework require specified entities to report certain cyber incidents to CERT In within a fixed time window after noticing them or being notified (Indian Computer Emergency Response Team, 2022). This governance logic treats speed of reporting as essential for containment and response. That logic mirrors the lived reality of cyber financial fraud, where early reporting can increase the probability of freezing or tracing funds (Indian Computer Emergency Response Team, 2022; Reserve Bank of India, 2017).

At the international level, UNODC frames cybercrime as a governance challenge requiring coordinated action by states, the private sector, and international cooperation mechanisms, because harms are layered and responses require legal, technical, and cooperative capacity (United Nations Office on Drugs and Crime, 2013). This reinforces the rationale for analysing governance texts, since they serve as vehicles through which coordination priorities and institutional responsibilities are communicated (United Nations Office on Drugs and Crime, 2013).

Policy texts, victim positioning, and secondary victimisation risk

A recurring concern in victimology is that institutional responses can deepen harm through blame, procedural burden, and uncertainty. In cyber fraud contexts, secondary harms may emerge through repeated narration requirements, complex evidence demands, opaque timelines, and victim blaming communication. Qualitative evidence suggests victims value clarity, validation, and practical guidance, especially in the early period after the incident when stress is high and cognitive load is constrained (Cross et al., 2016). Evidence synthesis also indicates that shame and fear of judgement can suppress reporting, which makes non stigmatising language and victim affirming pathways particularly important (Blakeborough & Gira Correia, 2018).

This makes framing central. Texts that construct victims primarily as careless users can amplify stigma and silence. Texts that construct victims as legitimate complainants who deserve assistance can lower reporting barriers and strengthen cooperation. A content analysis focus is therefore justified, because governance texts define both the problem and the socially acceptable response, including who is responsible, what victims should do, and what institutions promise to do in return (United Nations Office on Drugs and Crime, 2013).

Qualitative content analysis as an approach

Qualitative content analysis is a widely used method for interpreting meaning from textual data, and it can be implemented through multiple approaches that differ in how codes are developed and applied. Hsieh and Shannon (2005) describe conventional, directed, and summative approaches, and clarify that key distinctions include the origin of codes, the analytic procedures, and threats to trustworthiness (Hsieh & Shannon, 2005). Schreier (2012) provides practical guidance for building and testing a coding frame, segmenting text, trial coding, and iteratively refining categories to support analytic rigour and transparency (Schreier, 2012). Krippendorff (2019) conceptualises content analysis as a method for drawing replicable and valid inferences from texts to their contexts of use, and emphasises disciplined unitisation, explicit coding rules, and attention to meaning in context (Krippendorff, 2019).

In the present study, these methodological foundations justify a structured and auditable approach to analysing cybercrime governance texts. They also align with the study aim, which is not to estimate prevalence, but to map how harm, victimhood, responsibility, and coordination are constructed within authoritative narratives (Hsieh & Shannon, 2005; Schreier, 2012; Krippendorff, 2019).

METHODOLOGY

Study design

This study used qualitative content analysis to examine how cyber enabled financial fraud is framed in authoritative governance texts. Qualitative content analysis is suitable when the objective is to interpret patterned meanings, priorities, and silences within documents in a systematic and transparent way (Hsieh & Shannon, 2005; Krippendorff, 2019; Schreier, 2012). The study followed a directed approach, where the initial coding structure was guided by the research questions, and an inductive layer was added to capture recurring frames not anticipated in advance (Hsieh & Shannon, 2005).

Corpus and data sources

The corpus consisted of 20 publicly accessible documents that shape cyber fraud reporting, triage, liability, incident governance, and remedy. To ensure balance and coverage across the cyber fraud response ecosystem, documents were purposively sampled from four categories.

1. Policy and policing guidance, including national reporting guidance, operational advisories, and law enforcement focused documents.
2. Regulatory and banking texts, including consumer protection guidance, liability rules, and cyber security governance frameworks linked to banking and digital payments.
3. Incident governance and compliance texts, including mandatory incident reporting directions and associated clarifications for regulated entities.
4. Global benchmark reports from reputable international bodies, included only to contextualise dominant fraud mechanisms and governance trends.

The corpus was treated as a governance narrative dataset rather than as a measure of prevalence. The unit of inference was the framing and institutional logic expressed through the documents.

Inclusion and exclusion criteria

Documents were included if they met all the following criteria.

1. The text explicitly addressed cyber enabled financial fraud, unauthorised digital transactions, impersonation, phishing, payment fraud, or closely related reporting and remedy mechanisms.

2. The issuing body had formal authority or responsibility, such as a ministry, regulator, national reporting system, incident response authority, or an internationally recognised intergovernmental or law enforcement reporting body.
3. The document contained substantive framing or guidance, such as definitions, duties, reporting steps, timelines, liability allocation, coordination expectations, or remedy pathways.
4. The document was publicly available in English or available through an official translation.

Documents were excluded if they were purely technical standards with no linkage to crime response, reporting, victim experience, or institutional responsibilities, or if they were duplicates or superseded versions without added analytic value (Schreier, 2012).

Sampling strategy and saturation logic

Purposive sampling was used to select high influence texts that actively shape institutional practice and public reporting expectations. Sampling aimed for coverage across the full response chain, citizen reporting entry points, law enforcement workflows, banking liability rules, payment system security expectations, and entity level incident reporting norms. Saturation was assessed during coding, where additional documents were considered redundant when they repeated existing frames without introducing new categories or contradictions (Guest et al., 2006; Schreier, 2012). Although the corpus was fixed at 20 documents for feasibility and coherence, saturation checks were applied to confirm that major themes stabilised across categories.

Document management and corpus register

Each document was assigned a unique identifier, D01 to D20, and logged into a corpus register containing issuing body, year, document category, document type, and sections analysed. Documents were stored as PDF or text files, with version notes recorded when a document had a revised or updated edition. This created an audit trail and supported replicability of the corpus decisions (Krippendorff, 2019; Schreier, 2012).

Unit of analysis and context unit

The unit of analysis was the meaning unit, defined as a sentence, paragraph, clause, or numbered instruction that conveyed a complete idea relevant to the study aims. Examples include a liability rule, a reporting timeline, a citizen instruction sequence, or a statement allocating responsibility to an institution. The context unit was the surrounding section and headings needed to interpret the meaning unit correctly, particularly where procedural steps were embedded within longer operational guidance (Krippendorff, 2019; Schreier, 2012).

Coding framework development

A hybrid codebook was developed using both deductive and inductive procedures (Hsieh & Shannon, 2005).

Deductive code families were derived from the research questions.

1. Definition and scope of cyber enabled financial fraud

2. Harm framing, financial, trust related, psychological, social
3. Victim positioning, legitimacy, vulnerability, responsibility cues, blame cues
4. Offender and mechanism framing, social engineering, impersonation, technical enablers
5. Reporting pathway framing, first action clarity, channels, timelines
6. Responsibility allocation, police, banks, regulators, incident authorities, platforms
7. Coordination and workflow framing, handoffs, escalation, fragmentation indicators
8. Evidence and documentation burden, realism of expectations
9. Remedy and recovery framing, freeze, reversal, liability, compensation, updates
10. Tone and messaging stance, supportive versus blame leaning language

Inductive codes were added during initial coding when recurring frames emerged that were not captured by the deductive structure, such as procedural fatigue signals, implicit futility cues, or conflicting guidance across institutions (Hsieh & Shannon, 2005).

Coding and analysis procedure

Analysis was conducted in three stages.

Stage 1, familiarisation and memoing. Each document was read in full and summarised through analytic memos noting its dominant framing, implied responsibilities, and notable omissions.

Stage 2, first cycle coding. Meaning units were coded using the hybrid codebook. Multiple codes were permitted for a single meaning unit when the segment addressed more than one analytic domain, such as reporting timelines and victim responsibility cues.

Stage 3, second cycle synthesis. Codes were clustered into higher order categories and themes. Themes were refined by comparing patterns across the four document categories, which allowed identification of convergences, divergences, and institutional silences. Theme definitions were finalised when they met internal coherence, clear boundaries from other themes, and explanatory value for the research questions (Schreier, 2012).

Coding was carried out either manually or using qualitative analysis software. In either approach, the coding frame and audit trail were maintained to ensure transparency (Schreier, 2012).

Trustworthiness and rigour

Rigour was strengthened through established trustworthiness procedures (Lincoln & Guba, 1985; Nowell et al., 2017).

Audit trail was maintained through the corpus register, version notes, memos, and codebook revisions.
Triangulation was applied by comparing themes across policy, regulatory, incident governance, and benchmark documents, reducing dependence on any single institutional narrative. Negative case analysis was used by actively searching for documents that contradicted dominant frames, such as texts that explicitly recognise psychosocial harms or provide

integrated workflows, then using those cases to refine claims (Lincoln & Guba, 1985). Reflexive memoing documented analytic decisions and assumptions during coding to reduce unexamined bias in interpretation (Nowell et al., 2017). If required by the journal, a second coder can independently code a small subset of documents, followed by discussion and refinement of definitions. The study prioritised interpretive alignment over purely numeric reliability because meaning and context are central in governance text analysis (Krippendorff, 2019).

Ethical considerations

The study analysed publicly available documents and did not involve human participants, so informed consent was not applicable. Ethical care was applied by avoiding reproduction of victim blaming language without critical framing, and by presenting institutional critique in a balanced way grounded in observable textual patterns. Where examples could amplify harmful scripts, the study prioritised paraphrase over extended quotation while preserving analytic meaning.

FINDINGS

Corpus register D01 to D20

Doc ID	Issuing body	Year	Document title	Document type	Scope	Inclusion rationale for this study	Key sections analysed	Access link
D01	RBI	2017	Customer Protection, Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (Reserve Bank of India)	Circular notification	India, regulated banks	Core governance text for liability, reporting timelines, and victim protection framing	Liability rules, reporting windows, reversal timelines, customer communication	https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336
D02	RBI	2017	Customer Liability in Unauthorised Electronic Banking Transactions, SMS and IVRS awareness page (Reserve Bank of India)	Public awareness text	India, general public	Captures how "responsibility" is communicated to citizens, and how reporting urgency is framed	Awareness messaging, reporting prompt, channel design	https://www.rbi.org.in/commonman/english/Scripts/SMSLimitedliability.aspx
D03	RBI	2016	Cyber Security Framework	Regulatory framework notification	India, banks	Defines institutional duties for	Governance expectati	https://www.rbi.org.in/com

			in Banks (Reserve Bank of India)			detection, response, recovery, containment	ons, controls, incident management, oversight	monperson/English/Scripts/Notification.aspx?Id=1721
D04	RBI	2016	Annex to Circular on Cyber Security Framework in Banks (incident reporting template and fields) (Reserve Bank of India)	Annex, reporting schema	India, banks	Operationalises incident reporting and what counts as actionable information	Incident fields, timelines, reporting destinations, RCA elements	https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT41802062016.pdf
D05	CERT In, MeitY	2022	Directions under section 70B(6) on information security practices and cyber incident reporting (CERT-In)	Statutory directions	India, specified entities	Sets mandatory incident reporting norms and compliance duties, key governance narrative on speed	Reportable incidents, time limits, log retention, reporting procedures	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
D06	PIB	2022	Press release, CERT In issues directions for safe and trusted internet (Press Information Bureau)	Official press communication	India, public facing	Shows how the state justifies and frames compliance, gaps, and intended outcomes	Problem framing, rationale, implementation framing	https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904
D07	PIB	2022	Press release, FAQs on CERT In Cyber Security Directions and reporting expectations (Press Information Bureau)	Official press communication	India, public facing	Clarifies interpretive guidance and signals what “counts” as reportable	FAQ framing, incident categories, compliance emphasis	https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1826388
D08	CERT In	-	Guidelines on Information Security	Guidance document	India, govt entities	Captures public sector baseline	Preventive controls, response	https://www.cert-in.org.in/PDF/guid

			Practices for Government Entities (CERT-In)			controls and response norms	workflow, roles and responsibilities	elinesgovtentities.pdf
D09	NCRP, MHA	2019	Citizen Manual for reporting other cybercrimes (Report Other Cyber Crime workflow) (Cybercrime.gov.in)	User manual	India, citizens	Defines reporting pathway design and what information is demanded from victims	Stepwise reporting, fields, categories, evidence prompts	https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf
D10	NCRP, MHA	-	Citizen Financial Cyber Frauds Reporting instructions (what to do, where to report) (Cybercrime.gov.in)	Instruction sheet	India, citizens	High relevance to "golden hour" reporting narrative and victim routing	Helpline and portal steps, victim inputs, bank coordination cues	https://cybercrime.gov.in/UploadMedia/instructions_citizenreportingcyberfrauds.pdf
D11	NCRP, MHA	-	Financial Fraud Brochures, cyber safety and fraud reporting guidance (Cybercrime.gov.in)	Public awareness brochure	India, citizens	Captures prevention heavy framing, victim messaging, and recommended actions	Scam typologies, do and do not guidance, reporting prompts	https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf
D12	I4C, MHA	2024	Advisory to LEAs regarding Online Financial Frauds (Puducherry Police)	Law enforcement advisory	India, policing	Operational governance of freezing, coordination, and investigative priorities	Process guidance, coordination points, evidence needs, timelines	https://police.py.gov.in/Advisory%20to%20LEAs%20regarding%20Online%20Financial%20Fraud.pdf
D13	CEIB and stakeholders, circulated via	2024	SOP for information sharing with Law Enforcement Agencies	SOP	India, banks and LEA	Core coordination text, defines what data moves,	Data request workflow, formats, timefram	https://police.py.gov.in/Cyber%20Crime%20-%20I4C

	I4C context		(financial institutions to LEA) (Puducherry Police)			when, and how, reduces friction	es, points of contact	%20-%20Standard%20Operating%20Procedure%20%28SOP%29%20for%20Financial%20Institutions%20to%20LEA%20-%202024.pdf
D14	I4C, MHA	2024	I4C Daily Digest, 17.01.2024 (Indian Cybercrime Coordination Centre)	Bulletin digest	India, public facing	Shows the routinised narrative of threat, typologies, and enforcement actions	Incident typologies, institutional response cues, awareness framing	https://i4c.mha.gov.in/cyber_digest/jan_2024/I4C%20Daily%20Digest-%2017.01.2024%20.pdf
D15	PIB, MHA	2025	Curbing Cyber Frauds in Digital India (official note style PDF) (Press Information Bureau)	Government document	India, policy overview	Synthesises government framing of NCRP, 1930, capacity building, and outcomes	Institutional positioning, portal logic, capacity building narrative	https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/oct/doc2025107659501.pdf
D16	NPCI	2025	Mobile Application Security Framework, NPCI circular copy (rscb.bank.in)	Payments security framework	India, UPI ecosystem	Captures platform side responsibilities, compliance and audit logic for fraud prevention	App security controls, compliance requirements, audit expectations	https://rscb.bank.in/Content/pdf/npcicircular.pdf
D17	WEF	2025	Fighting Cyber Enabled Fraud, A Systemic	Global policy report	Global	Provides comparative framing, ecosystem responsibili	Ecosystem model, signal sharing, incentives	https://reports.weforum.org/docs/WEF_Fight

			Defence Approach (reports.weforum.org)			ties, and systemic prevention concepts	, cross sector response	ing_Cyber-Enabled_Fraud_2025.pdf
D18	FBI IC3	2024	2024 IC3 Annual Report (Internet Crime Complaint Center)	Annual report	United States, global victim intake relevance	Benchmark evidence on dominant scam types, losses, and vulnerable groups	Typologies, complaint volumes, loss distribution, victim demographics	https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
D19	Europol	2024	Internet Organised Crime Threat Assessment (IOCTA) 2024 (Europol)	Threat assessment	EU	Benchmark on organised online fraud, techniques, and enforcement implications	Threat trends, fraud ecosystem, enablers, response implications	https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
D20	Reuters	2026	RBI plans customer compensation framework for small value digital payment frauds (Reuters)	News report of policy announcement	India	Captures the newest governance direction, compensation framing, and responsibility allocation	Remedy framing, eligibility logic, proposed safeguards, policy justification	https://www.reuters.com/world/india/india-central-bank-propose-framework-compensate-customers-digital-payment-frauds-2026-02-06/

Findings

Theme 1. Cyber enabled financial fraud is constructed as a high volume deception ecosystem, not a purely technical intrusion problem

Across global benchmark reports and Indian institutional texts, cyber enabled financial fraud is framed primarily as an offence of deception, persuasion, and impersonation that scales through low effort and high reach tactics. In the global corpus, FBI Internet Crime Complaint Center reporting and Europol assessment texts present phishing or spoofing and investment fraud as dominant categories by volume or losses, and they emphasise fraud schemes that rely on social engineering and trust manipulation rather than sophisticated system exploitation (D14 to D16).

Indian governance texts mirror this logic by repeatedly foregrounding typologies such as impersonation, caller spoofing, and payment fraud narratives, and by positioning citizen awareness and rapid reporting as central prevention levers (D07 to D13).

Interpretive synthesis: The corpus consistently constructs the fraud problem as an industrialised persuasion market where speed and scale matter as much as technical capability. This framing implicitly shifts the policy emphasis toward early interruption and coordinated response, rather than only hardening systems.

Theme 2. Speed is framed as the main determinant of outcome, creating a governance logic of the "golden hour"

A strong and consistent theme across Indian reporting and response documents is that time is the key control variable. The National Cybercrime Reporting Portal and related system pages emphasise immediate reporting through helpline 1930 and the portal, signalling that early action is necessary for possible fund holds and restoration workflows (D07, D10, D11).

This time critical framing is reinforced in operational law enforcement guidance. The advisory to law enforcement agencies stresses rapid routing of complaints and quick coordination with financial intermediaries, presenting delay as a structural risk that reduces the probability of freezing or tracing funds (D08).

Parallel urgency appears in compliance oriented cyber incident governance. CERT-In directions require specified entities to report listed cyber incidents within a fixed time window after noticing or being notified, which institutionalises speed as a compliance norm at the organisational level (D04, D05, D06).

Interpretive synthesis: The corpus treats early reporting not merely as good practice but as a functional technology of containment. The broader governance narrative implies that once instant payment rails complete transfers and money moves through layered accounts, response shifts from prevention to post hoc investigation, with sharply reduced recovery prospects.

Theme 3. Reporting pathways are multi entry but not always integrated into a single coherent victim journey

Citizen facing texts repeatedly provide multiple entry points, especially helpline based reporting and portal based reporting. The portal landing pages and reporting instructions foreground access and immediacy, using simple prompts that prioritise complaint registration (D07, D11).

At the same time, the corpus shows that multi entry systems can introduce pathway ambiguity. The portal itself carries a stated focus on cyber crimes against women and children, while separately promoting financial fraud reporting via 1930, which can create a split mental model for citizens about where financial fraud fits, and which workflow applies (D07, D12).

Institutional texts from Indian Cyber Crime Coordination Centre present the Citizen Financial Cyber Frauds Reporting and Management System as the backend logic for quick reporting and action, suggesting a workflow intent, but the public narrative still reads as a set of channels rather than a clearly staged journey from first action to resolution (D10).

Interpretive synthesis: The corpus constructs reporting as urgent and accessible, but it is less consistent in presenting a single end to end victim journey. This creates room for confusion about sequencing, evidence expectations, and what outcomes can realistically be expected after reporting.

Theme 4. Responsibility is distributed across institutions, but citizen facing messaging often recentres the burden on individual vigilance

Regulatory and governance texts allocate responsibility across multiple institutional actors. Reserve Bank of India circulars position banks as responsible for immediate steps after notification and for implementing customer protection rules on liability limitation in unauthorised electronic transactions, tying outcomes partly to timeliness of reporting and bank side action (D01).

Cyber incident governance texts allocate duties to service providers, intermediaries, and organisations through mandatory reporting and log retention expectations, reinforcing that institutions, not only citizens, have defined obligations in the incident response ecosystem (D04, D05).

Payment system and UPI security frameworks focus on ecosystem level controls, compliance mandates, and audit mechanisms, signalling that fraud reduction is also an infrastructural and governance task, not merely a user behaviour task (D12, D13).

In contrast, public guidance and awareness materials frequently foreground user behaviour controls such as not sharing OTPs and being cautious, which is important for prevention, but can also create an implicit narrative where the victim's primary role is to avoid mistakes and comply quickly, rather than to be supported through a predictable response pathway (D07, D09, D11).

Interpretive synthesis: The governance architecture in the corpus is multi actor and institution heavy, but the public facing narrative often compresses this complexity into individual vigilance plus fast reporting. This can obscure system responsibilities and may contribute to self blame in victims, particularly when recovery is not achieved.

Theme 5. Remedy and victim protection are operationalised mainly through liability rules, compensation logic, and system trust preservation

The most concrete victim protection instrument in the Indian corpus is the RBI liability limitation framework, which sets expectations about customer liability and bank obligations for unauthorised electronic banking transactions (D01).

A newer policy direction, reported through Reuters, indicates a move toward a compensation framework for small value digital payment fraud, explicitly framed as providing immediate relief and reinforcing trust amid high frequency fraud exposure (D19).

Payment system governance texts also emphasise security, resilience, and reliability as ecosystem objectives, which implicitly positions consumer protection as a trust sustaining function within a mass adoption payment environment (D12, D13).

Interpretive synthesis: Victim protection is framed predominantly as financial remedy, liability allocation, and system trust maintenance. Psychosocial recovery and support needs appear comparatively marginal as explicit governance commitments.

Theme 6. Psychosocial harms, stigma, and secondary victimisation risks are weakly articulated compared to procedural and compliance priorities

Across the corpus, harms are primarily rendered as financial loss, systemic risk, and trust impacts. Direct references to distress, shame, anxiety, or longer term psychosocial disruption are limited in the governance documents examined, especially compared to the density of procedural instructions, reporting timelines, and compliance duties (D01, D04, D07, D08, D10 to D13).

Global benchmark texts acknowledge scale and typologies, and they underline large losses and concentration of harm in older adults, but they too focus more on incident categories and economic loss than on recovery oriented victim support pathways (D14 to D16).

Interpretive synthesis: The corpus is rich in administrative rationality, speed, channels, duties, compliance, and remedy rules, but relatively thin in explicit victim centred recovery language. This imbalance indicates a governance narrative that treats victims primarily as reporters and consumers, rather than as persons experiencing multi layer harms who may require supportive communication, reassurance, and structured follow up.

Cross theme summary

1. Rapid reporting and rapid coordination as the core recovery lever. (D07, D08, D10, D11)
2. Institutional duties framed through compliance, liability rules, and ecosystem security mandates. (D01, D04, D12, D13)
3. Fraud framed as scalable deception, with phishing and investment fraud repeatedly treated as major drivers. (D14 to D16)
4. Comparatively limited articulation of psychosocial harm and recovery support as governance obligations. (Across corpus)

DISCUSSION

This qualitative content analysis shows that contemporary cyber enabled financial fraud governance is organised around three linked logics, deception at scale, speed as outcome determinant, and remedy framed through liability and trust preservation. At the same time, the corpus gives comparatively limited explicit space to psychosocial harm, stigma, and recovery support, even though victimology evidence consistently shows that fraud produces distress, shame, anger, self blame, and longer term disruption (Button et al., 2014; Cross et al., 2016). The discussion below interprets what these patterns mean for policy design, institutional practice, and victim outcomes.

Deception led fraud reframes “security” as a communication and workflow problem

Across the corpus, fraud is repeatedly constructed as a persuasion ecosystem rather than a purely technical intrusion problem. This aligns with international evidence that complaint volumes are dominated by phishing and impersonation, and that high loss categories such as investment scams rely heavily on social engineering (Federal Bureau of Investigation, Internet Crime Complaint Center, 2024; Europol, 2024). The implication is that cyber fraud control cannot be treated only as a cybersecurity hygiene task. It is also a public communication, consumer protection, and workflow engineering task.

In this framing, offenders exploit authority cues, urgency cues, and perceived legitimacy, which compresses decision time and shifts victimisation into a narrow window of coerced compliance. This supports the argument that victimisation is not adequately explained by carelessness alone, because the offence is designed to reduce deliberation and verification (United Nations Office on Drugs and Crime, 2013). A governance narrative that over emphasises vigilance may unintentionally strengthen self blame and reduce reporting propensity, consistent with evidence that shame and embarrassment are important barriers to reporting (Blakeborough & Gira Correia, 2018; Cross et al., 2016).

The “golden hour” logic is coherent, but the citizen journey is not always made coherent

A clear strength of the Indian governance texts is their shared emphasis on speed. Reporting channels and operational advisories construct early reporting as the most important lever for freezing and tracing funds, which is logically consistent in instant payment environments. This time centric logic echoes institutional compliance narratives in CERT-In directions and aligns with the operational governance focus in I4C guidance.

However, the corpus also suggests that the citizen facing narrative is often channel centric rather than journey centric. When citizens are given multiple entry points without a single staged explanation of what happens next, when banks are contacted, what evidence is minimally required, what timelines are realistic, and how updates will be delivered, reporting can still feel futile even when access is available. This matters because perceived futility is a core driver of underreporting in fraud contexts (Blakeborough & Gira Correia, 2018). A system can be fast on paper, but still feel opaque to victims, which increases withdrawal, repeat narration, and secondary distress (Cross et al., 2016).

Responsibility is distributed in governance, but responsibility is individualised in public messaging

The corpus distributes responsibilities across policing, banking, payment systems, and incident governance. This is visible in Reserve Bank of India customer protection rules, NPCI security frameworks, and compliance obligations in CERT-In texts. Yet public facing guidance frequently re centres the narrative on individual vigilance and fast compliance, such as OTP warnings and do and do not lists.

This creates a subtle imbalance. The governance architecture is multi actor, but the social meaning of fraud risk can become moralised, where the victim’s error is foregrounded more than system responsibilities and service standards. Victimology research indicates that shame and fear of being blamed can suppress reporting, especially for fraud where victims already question their own judgement (Button et al., 2014; Cross et al., 2016). Therefore, a key implication is that prevention messaging should be paired with explicit anti blame and support language. This is not only ethical, it is operationally useful because it can increase timely reporting and improve recovery odds.

Remedy is framed mainly as liability and compensation, which protects trust but may narrow recovery

The corpus positions remedy primarily through liability limitation, dispute handling, and compensation logic, which is consistent with a consumer protection framing of digital finance. The presence of liability caps and proposed compensation for small value frauds, as described in Reuters coverage, signals an institutional concern with sustaining trust and adoption in digital payments. This trust stabilisation objective is also visible in ecosystem security texts and governance narratives.

Yet the same focus can narrow the meaning of recovery. Victim recovery in fraud includes financial loss, but also emotional stabilisation, reassurance, clarity, and restoration of confidence in institutions (Button et al., 2014; Cross et al., 2016). When texts rarely articulate these dimensions, there is a risk that institutional responses treat victims primarily as transaction cases. This can unintentionally intensify secondary victimisation through opaque timelines, repeated documentation demands, and blame leaning communication. These are well known stress multipliers in fraud reporting experiences (Cross et al., 2016).

Underreporting is treated as friction and incentives, but stigma and trauma are under addressed

The corpus implicitly supports a rational choice account of reporting where friction, benefit calculations, and system capacity shape reporting. This is compatible with evidence reviews that highlight perceived futility and complexity as key barriers (Blakeborough & Gira Correia, 2018). However, the relative silence around shame and self blame indicates a gap between what victims experience and what governance texts explicitly acknowledge. Addressing this gap is practical, not sentimental. It affects reporting speed, cooperation, evidence quality, and sustained engagement.

Limitations and future research

This study analyses governance texts and does not measure prevalence or victim outcomes directly. Text selection may privilege nationally visible documents and English language materials, which can under represent local practices and regional language guidance. Future research should triangulate these findings with victim interviews, complaint pathway observation, and stakeholder interviews across police, banks, payment operators, and regulators to test how governance framing translates into practice and how it shapes reporting speed, cooperation, and recovery outcomes (Hsieh & Shannon, 2005; Schreier, 2012).

Conclusion

This study analysed a purposive corpus of 20 authoritative governance texts to examine how cyber enabled financial fraud is constructed within institutional narratives. The findings show that the dominant framing positions cyber financial fraud as a scalable deception ecosystem, where persuasion and impersonation tactics drive high volume victimisation. Across Indian reporting and response texts, speed emerges as the central governance variable, with early reporting and rapid inter institutional coordination framed as the primary determinants of recovery potential. At the same time, while responsibilities are distributed across police, banks, payment systems, and incident authorities within formal governance architecture, public facing guidance often recentres the burden on individual vigilance and reporting compliance.

The study also finds that victim protection is operationalised mainly through liability limitation, dispute handling, and compensation logic, reflecting a consumer protection and trust preservation orientation. However, psychosocial harms, stigma, and secondary victimisation risks receive limited explicit attention relative to procedural and compliance priorities. The paper therefore contributes a governance framing insight, that the effectiveness of cyber fraud response is shaped not only by technical controls and legal mandates, but also by how texts communicate victim legitimacy, clarify an end to end reporting journey, and set realistic expectations for evidence, timelines, and follow up. Strengthening these narrative and workflow elements can improve timely reporting, reduce underreporting driven by shame and futility, and support recovery that includes both financial remedy and restoration of confidence in institutions.

REFERENCES

Blakeborough, L., & Gira Correia, S. (2018). *The scale and nature of fraud: A review of the evidence*. Home Office.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36–54.

Cross, C., Richards, K., & Smith, R. G. (2016). *The reporting experiences and support needs of victims of online fraud* (Trends & Issues in Crime and Criminal Justice No. 518). Australian Institute of Criminology.

Europol. (2024). *Internet organised crime threat assessment (IOCTA) 2024*

Federal Bureau of Investigation, Internet Crime Complaint Center. (2024). *Internet crime report 2024*

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59–82.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277–1288.

Indian Computer Emergency Response Team. (2022, April 28). *Directions under sub section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted Internet*.

Indian Computer Emergency Response Team. (n.d.). *Guidelines for information security practices for government entities*

Indian Cyber Crime Coordination Centre. (2024, April 29). *Advisory to law enforcement agencies regarding online financial fraud*

Indian Cyber Crime Coordination Centre. (2024, January 17). *I4C daily digest*

Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). SAGE.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE.

Ministry of Home Affairs. (2019). *Citizen manual for reporting other cyber crimes on the National Cyber Crime Reporting Portal*

Ministry of Home Affairs. (2025, December 2). *Lok Sabha Unstarred Question No. 452, Answer by Minister of State in the Ministry of Home Affairs*.

Ministry of Home Affairs. (n.d.). *Financial fraud brochures*

Ministry of Home Affairs. (n.d.). *Instructions for citizen reporting of financial cyber frauds*

National Payments Corporation of India. (2025, May 19). *Comprehensive mobile application security framework for UPI 2025*

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13.

Press Information Bureau. (2022, April 28). *CERT In issues directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted internet*.

Press Information Bureau. (2022, May 20). *FAQs on CERT In cyber security directions and reporting requirements*.

Press Information Bureau. (2025). *Curbing cyber frauds in Digital India*

Reserve Bank of India. (2016, June 2). *Annexure to circular on cyber security framework in banks*

Reserve Bank of India. (2016, June 2). *Cyber security framework in banks*.

Reserve Bank of India. (2017, July 6). *Customer protection: Limiting liability of customers in unauthorised electronic banking transactions* (RBI/2017–18/15).

Reserve Bank of India. (n.d.). *Customer liability in unauthorised electronic banking transactions, SMS and IVRS awareness message*.

Reuters. (2026, February 6). *India central bank to propose framework to compensate customers for small value digital payment frauds*.

Schreier, M. (2012). *Qualitative content analysis in practice*. SAGE.

Indian Cyber Crime Coordination Centre. (2024) *SOP for information sharing between financial institutions and law enforcement agencies in online financial fraud cases*

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*.

World Economic Forum. (2025). *Fighting cyber enabled fraud: A systemic defence approach*