KPMG

FICCI 100
100 YEARS OF BUILDING TOMORROW

Next-Gen Forensic

The new age of fraud investigation

June 2026

kpmg.com/in

KPMG. Make the Difference.

Table of Contents

Foreword by KPMG in India

Fraud has exploded into a full-scale enterprise – big enough to threaten reputations of companies and in some cases economies at large. What was once the domain of lone or select bad actors is now taking shape of an industry, costing the world billions of dollars annually and leaving citizens, boards and regulators grappling with unprecedented risks.

We read about customer data breaches, deepfake-driven scams, and brazen digital bank heists – but behind those headlines lies a stark reality: our traditional defenses, detection and investigation methods are struggling to keep pace with evolving developments in the field of technology and motivations behind evolving geo-politics where state actors are also at play.

As stewards of trust and corporate values, we must ensure that our organisation isn't the next cautionary tale. Doing so will require embracing transformative, evidence-led fraud defenses that are as agile and coordinated as the threats they counter. The message is clear: proactive Forensic readiness is now a leadership imperative.

FICCI and KPMG in India have come together to set out key insights into how to reinforce trust, bolster preventive, detective, investigative and remediation capabilities, and turn the tide against industrialised fraud. This report reveals where current approaches may need further strengthening and outlines considerations relevant to enabling a more resilient model. The future of our digital economy and growth depends on many components including getting this right.

Suveer Khanna
Partner and Head,
Forensic Services
KPMG in India

Foreword by FICCI

In an era where crime is increasingly technology-driven, borderless, and constantly evolving, Forensic investigation has emerged as a critical pillar of institutional resilience, national security, and digital trust. As India accelerates its journey toward becoming a leading global digital economy, the need for advanced and future-ready Forensic capabilities has become more important than ever. Modern Forensic frameworks now extend far beyond the traditional examination of devices and storage media, encompassing the ability to trace complex digital identities, reconstruct intricate activity trails, authenticate digital evidence with precision, and enable rapid, intelligence-led responses across interconnected ecosystems. In today's dynamic digital landscape, the ability to identify, preserve, analyse, and act upon digital evidence is fundamental to combating sophisticated crime, safeguarding consumers, and reinforcing confidence in digital systems. As threats continue to grow in sophistication and scale, robust Forensic readiness is no longer merely an investigative necessity but a strategic imperative for ensuring accountability, strengthening organisational resilience, and securing India's digital future.

The FICCI–KPMG in India report, examines the evolving landscape of crime and the growing importance of Forensic readiness across sectors. It highlights how investigative frameworks must evolve alongside emerging technologies, payment ecosystems, and fraud methodologies.

At FICCI, we believe that strengthening digital trust requires sustained collaboration between industry, regulators, law enforcement agencies, and technology stakeholders. I am sure that this report will serve as a valuable resource for the broader investigative and policy ecosystem, as India prepares to address next-generation crime and evolving Forensic challenges.

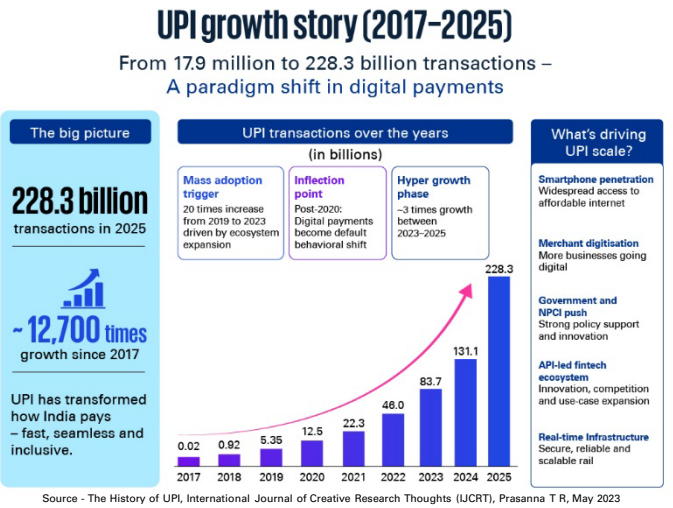
Jyoti Vij
Director General
FICCI

Executive summary

Fraud has entered a new phase. It is no longer confined to false claims, forged documents, isolated payment diversion, or traditional internal misconduct. Fraud now operates as a digitally enabled ecosystem that exploits stolen data and identities, real-time payment infrastructure, social media platforms, mule-account networks and increasingly artificial intelligence. Mass smartphone adoption and app-based digital banking have expanded access to financial and public services at scale. India alone grew from 25 crore internet connections in 2014 to over 100 crore by 2025, while average monthly data consumption per wireless data subscriber rose 399 times to 24.01 GB in 2025. Cyber fraud risks have grown alongside this digital expansion.[1]

Recent global threat reports indicate that cyber-enabled fraud is scaling across sectors, globally increasingly becoming more organised, more transnational, and more difficult to investigate using traditional methods. For example, Europol's 2025 Internet Organised Crime Threat Assessment and INTERPOL's 2026 Global Financial Fraud Threat Assessment underscore that today's fraud attack surface spans stolen credentials, application programming interface (API) abuse, software-as-a-service (SaaS)/cloud compromise, social engineering, third-party supply-chain vulnerabilities, and specialised criminal service providers.[2] Organised cybercrime thrives on stolen identities and personal data, weaponising them at industrial scale. Criminal syndicates exploit troves of leaked personally identifiable information (PII) and even pre-activated SIM card networks to impersonate victims and launder illicit gains. India recently cancelled 12 lakh fraudulent SIMs and blocked three lakh device IDs, i.e., international mobile equipment identity (IMEI) numbers, in a single nationwide crackdown.[3] Europol describes online fraud schemes as the fastest-growing area of organised crime, notes that these schemes are now run as 'highly efficient, transnational industries', and reports more than 120 active ransomware brands observed in 2025.[2] Call-centre scam factories, often run with trafficked 'cyber-slaves' in Southeast Asia, are defrauding victims worldwide with impunity; in 2025, Americans alone suffered USD7.2 billion in reported losses to cryptocurrency investment frauds emanating from the region.[4] These transnational fraud nodes leverage anonymity across borders and relocate when raided, outpacing law enforcement and dragging out legal action.

In India, this shift is occurring alongside large-scale digital payment adoption. Government reporting notes that Unified Payments Interface (UPI) processed over 24,162 crore transactions valued at approximately INR314 lakh crore in FY 2025–26, approximately USD3.3 trillion — comparable to the combined economic output of countries such as Australia and Mexico or Spain and South Korea— and accounted for about 85 per cent of India's digital payments volume in FY 2025–26.[5] In parallel, Ministry of Home Affairs (MHA) reporting through the National Cyber Crime Reporting Portal (NCRP)/Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) records 24,02,579 online financial fraud complaints in 2025 with an amount reported of INR22,495 crore; the CFCFRMS mechanism reported saving more than INR8,189 crore up to 31 December 2025.[6] This combination of scale and velocity expands the attack surface for impersonation, mule routing, account takeover, beneficiary manipulation, know your customer (KYC) abuse, and rapid financial movement, making resilience and recoverability core to the design of payment architectures, fraud controls, and regulatory oversight frameworks.



Source - The History of UPI, International Journal of Creative Research Thoughts (IJCRT), Prasanna T R, May 2023

Meanwhile, new digital channels create fresh attack vectors — fast e-commerce and logistics platforms, instant loans and trading apps — giving fraudsters new openings to exploit speed and trust dependencies. Extortion schemes, from sextortion to ransomware, proliferate; global cybercrime reports now rank online extortion among the top three threats by complaint volume, and thousands of ransomware attacks on smaller firms go under-reported as victims quietly pay modest sums to avoid drawn-out investigations.

[1] 2025 Year End Review for Department of Telecommunications, Department of Telecommunications, Ministry of Communications, December 2025, accessed 31 May 2026.
[2] Steal, deal and repeat – How cybercriminals trade and exploit your data: Internet Organised Crime Threat Assessment 2025, Europol, 2025; Global Financial Fraud Threat Assessment, INTERPOL, March 2026.
[3] 12 lakh SIM cards cancelled in cybercrime crackdown, The Cyber Express, February 2026; Department of Telecommunications takes strong action against telecom misuse through Sanchar Saathi portal, Press Information Bureau, Ministry of Communications, Government of India, March 2025.
[4] Cryptocurrency and AI scams bilk Americans of billions, Federal Bureau of Investigation, April 2026; New Scam Center Strike Force battles Southeast Asian crypto investment fraud targeting Americans, United States Secret Service, November 2025; Treasury sanctions Southeast Asian networks targeting Americans with cyber scams, U.S. Department of the Treasury, September 2025
[5] UPI completes 10 glorious years, emerges as world's largest real-time payments platform, anchoring India's digital economy, Press Information Bureau, Government of India, April 2026.
[6] Cyber frauds mount to Rs22,495 crore in 2025; over Rs8,000 crore saved through rapid response system, Dynamite News, February 2026; Indian Cybercrime Coordination Centre: National Cybercrime Reporting Portal and Citizen Financial Cyber Fraud Reporting and Management System, Ministry of Home Affairs, accessed 31 May 2026.

Executive summary

Today's threat actors are also innovating with artificial intelligence (AI), deploying deepfakes, voice cloning, and automated hacking tools to probe for systemic gaps — even malicious insiders and compromised suppliers can serve as vectors. This introduction sets the stage for the detailed analyses ahead by underlining the complex, evolving threat landscape: a world where digital opportunity and digital risk have grown in tandem, demanding urgent, coordinated vigilance from policy-makers and enterprises alike.

From sector analysis, in **banking, financial services and insurance (BFSI)**, fraud patterns are diverging — Reserve Bank of India (RBI) data show digital and card scams now account for two-thirds of bank fraud incidents by number, at 66.8 per cent, but under 10 per cent of losses, whereas a smaller share of high-value loan/credit frauds, at 19 per cent of cases, drive one-third of losses.[7] With recovery rates as low as approximately six per cent for digital payment frauds, the new reality is that proactive controls and rapid response count far more than after-the-fact redress.[8]

Within public **digital infrastructure**, scale is creating fraud asymmetry. Fraudsters use a maze of high transaction volume, mass QR acceptance, mobile-first access, and frictionless interoperability to their advantage. The RBI's move toward payee-name validation and India's Fraud Risk Indicator (FRI) model reflect a strong focus on identity trust scoring with pre-transaction risk signalling mechanisms. [9]

In the world of **virtual digital assets (VDAs)/crypto/Web3**, more than an exchange hack problem, crypto crime is increasingly a payments and sanctions problem. U.S. victims reported over USD11 billion in crypto-linked scam losses in 2025 as criminals exploit cryptocurrency for cross-border laundering and sanctions evasion using tools like stablecoins. The crypto risk now sits at the intersection of fraud, anti-money laundering and sanctions control. [10]

For the **automotive and industrial manufacturing (IM) sector**, interconnected systems have expanded attack surfaces from plant floors to entire ecosystems. In manufacturing, classic ransomware and credential abuse dominate, but in automotive, data show the important shift: backend, telematics, API, and cloud pathways now create 'one-to-many' operational risk, where a single breach can disable fleets or disrupt supply chains. Boards need to understand it as a business continuity and safety issue, and not just an information technology (IT) issue.

In **energy and utilities**, cyber incidents increasingly blend extortion with sabotage, elevating risks from financial loss to operational and physical safety in real time. This convergence requires boards and regulators to treat it as a core operational resilience and regulatory compliance issue rather than a standalone IT concern.

Government and public sector risk is now dual track: hostile external intrusion plus internal error at scale. Cyber risk in government is not only malware/ransomware attacks; it is also process error, mass mis-delivery, bad configuration, and PII exposure. This highlights the need for robust cyber fraud governance with strict security, quality operations, careful data management, and thorough vendor oversight.

Finally, for **e-commerce and gig economy**, fraud is moving 'upstream' into discovery and contact channels. In gig and job platforms, fraudsters increasingly target victims before transactions occur — the FBI's 2025 data show nearly 25,000 employment-related scam complaints, indicating that recruitment, onboarding, and identity verification are new frontlines for fraud prevention. Boards and regulators must therefore reinforce defences before payment is even in sight, focusing on trust and authenticity in user engagement channels.[11]

Against this background, the report argues that fraud investigation must evolve into 'next-generation forensic'. This means moving beyond traditional device-centric or post-loss reviews towards a broader investigative model that is identity-centric, cloud-aware, payment-aware, evidence-governed, and intelligence-led. It also means accepting that modern fraud rarely fits neatly into one category. A single incident may simultaneously involve cyber intrusion, social engineering, transaction manipulation, insider facilitation, third-party exposure, and laundering. Effective response therefore depends on the ability to correlate technical evidence, financial movement, communication trails, access events, and governance decisions into one defensible narrative.

[7] Report on Trend and Progress of Banking in India, Reserve Bank of India, December 2025.
[8] India Records INR805 crore in UPI frauds this fiscal year as government reveals alarming stats and low recovery rates, INVC, December 2025;
[9] DoT introduces "Financial Fraud Risk Indicator (FRI)" to strengthen cyber fraud prevention, Press Information Bureau, Department of Telecommunications, May 2025.
[10] Cryptocurrency and AI scams bilk Americans of billions, Federal Bureau of Investigation, April 2026; FBI 2025 Internet Crime Report, Federal Bureau of Investigation, 2026.
[11] 2025 Internet Crime Report, Internet Crime Complaint Center, Federal Bureau of Investigation, 2026.

Executive summary

First, **the fraud economy has become industrialised.** Data, credentials, access, and fraud tooling are now commodified across criminal ecosystems. Fraud is often enabled by specialisation; including reconnaissance, access brokerage, execution, laundering, and obstruction of recovery efforts may all be performed by different actors. This challenges the traditional notion of a single fraudster or an isolated event increasingly outdated.

Second, **the nature of evidence has changed.** Critical artefacts now reside across cloud platforms, identity providers, endpoints, mobile devices, payment systems, telecom metadata, audit logs, and third-party environments. Evidence is more volatile, more distributed, and more dependent on pre-existing system design choices such as logging depth, retention periods, and access rights. The quality of an investigation increasingly depends on forensic readiness established before the incident occurs.

Third, **institutional constraints remain a major weakness.** Many organisations still operate with siloed fraud, cyber, legal, and compliance teams, fragmented logging, weak preservation protocols, and insufficient 'case-to-control' learning loops. Law enforcement agencies face separate but related issues: speed mismatch, cross-border dependence, resource constraints, and evidence coordination challenges. The consequence is that attackers are often better aligned operationally than the institutions pursuing them.

Fourth, **regulatory direction** is pushing institutions toward stronger fraud governance. In India, the policy trend is toward secure onboarding, digital payment security, strengthened fraud reporting, improved customer protection, and more formal anti-fraud frameworks. More broadly, the global policy environment increasingly expects coordination across fraud prevention, anti-money laundering (AML), cyber resilience, and evidence quality. Institutions that treat fraud capability as a side function may find themselves under-prepared not only operationally but also from a governance and regulatory standpoint.

Fifth, the **solution is not simply better tooling.** It is better operating design. Next-generation forensic readiness requires trained people, evidence-aware processes, scalable analytic support, clear escalation criteria, secure case management, role clarity across functions, and structured post-incident learning. AI and automation can accelerate aspects of triage, lead identification, pattern analysis, media review, and anomaly detection, but they must be used within a governance model that supports explainability and evidentiary discipline.

The report therefore proposes a practical shift: from investigation as reaction to investigation as next-generation intelligence infrastructure. Fraud investigations should not end with case closure. They should generate, typologies, taxonomies, control improvements, monitoring rules, reskilling initiatives, governance lessons, regulatory alignment, and forensic design changes that reduce the impact of future incidents. Institutions that can do this consistently will be better placed to contain fraud losses, improve customer trust, support regulator engagement, and strengthen resilience across digital channels.

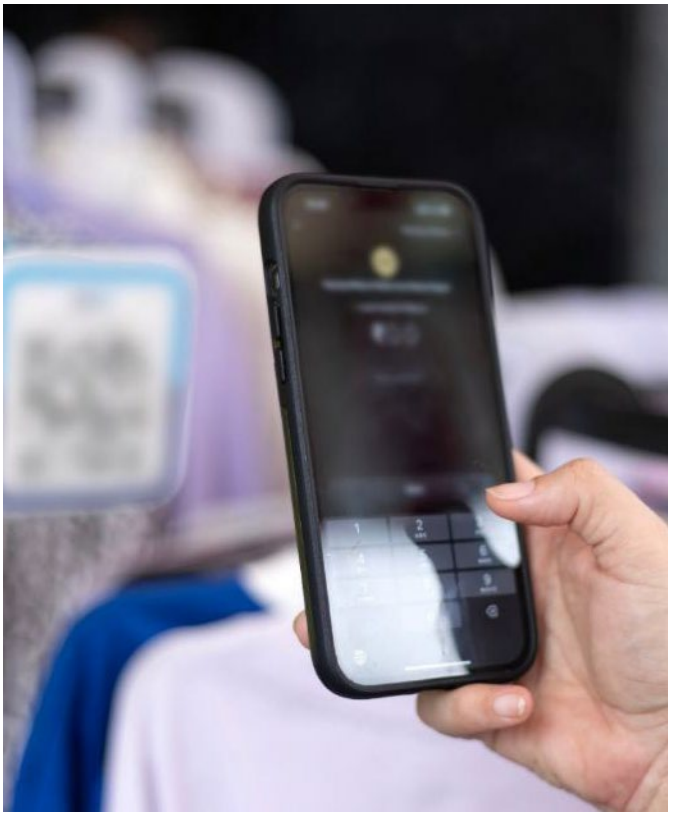
In conclusion, next-generation forensic is not merely an updated form of digital investigation. It is a strategic capability for the digital economy. As fraud becomes faster, more deceptive, and more distributed, organisations must build systems that preserve evidence, shorten decision cycles, and continuously convert incidents into intelligence. In the years ahead, the quality of this capability will increasingly shape not just investigative outcomes, but institutional credibility and resilience itself.

Chapter 1

Introduction

1. Introduction

This report examines how investigative intelligence and emerging technologies are shaping the fight against cyber-enabled financial crime and frauds in India's rapidly evolving digital economy. India's digital payments infrastructure is among the world's largest. What that scale creates, beyond economic efficiency, is a surface area for fraud that was structurally impossible 10 years ago. The challenge this report addresses is not that digital payments are inherently unsafe, they are not. Now the task is to expand our protective systems so that they keep pace with this success, reinforcing the trustworthiness of a platform that is fundamentally secure.



The scale shift is significant. UPI, launched in April 2016, now operates at national scale: Government reporting notes over 24,162 crore annual transactions and approximately INR314 lakh crore annual value in FY 2025–26, with monthly volumes crossing 2,000 crore transactions in 2025.[5] At this scale, fraud execution and fund dispersal can occur within minutes; effective defense therefore depends on rapid reporting, coordinated response, and evidence readiness across payment rails, identity systems, devices, and communication channels.

1.1 Evolving threat landscape

Rise of cyber-enabled financial frauds

Financial fraud has always existed. What has changed is the infrastructure available to perpetrate it and the speed at which losses accumulate. The complaint data from National Crime Records Bureau (NCRB) and Indian Cyber Crime Coordination Centre (I4C) confirm that payment fraud, encompassing UPI fraud, credit card skimming, and mobile banking takeovers, now accounts for the largest share of all cybercrime complaints by value.[12]

Phishing remains the most common initial access vector, but its character has shifted. Phishing, combined with AI-driven misinformation, bulk email infrastructure, subscriber identity module (SIM)-farms, and malicious advertising, has been successful in many cases as an attack vector, driving manipulation of victims into either connecting their bank accounts or wallets to malicious apps and smart contracts, or unknowingly approving transactions. This form of cyber fraud is replacing purely technical exploits. Smishing, i.e., SMS-based phishing, targeting OTP interception or leakage of secret information, continues to be a primary method for account takeover, particularly in the banking sector.

[12] Cyber Fraud and Digital Harassment, Press Information Bureau, Ministry of Home Affairs, December 2024; National Cybercrime Reporting Portal and Citizen Financial Cyber Fraud Reporting and Management System, Indian Cybercrime Coordination Centre, Ministry of Home Affairs, accessed 31 May 2026.

AI-enabled crime and deepfakes

Generative AI entered the financial crime toolkit at scale in 2023. The most widely documented application is voice cloning for CEO fraud: an executive's voice is synthesised from publicly available recordings and used to instruct a finance officer to execute an urgent payment. Several cases in India's manufacturing sector have involved this method, with material financial losses reported to enforcement agencies. In Singapore, in a documented case, a victim lost approximately USD3.8 million after being deceived through a sophisticated deepfake video conferencing scam that impersonated senior government authorities.[13]

On the defensive front, the Reserve Bank of India (RBI) Annual Report 2024–25 highlights the deployment of MuleHunter.AI — an advanced artificial intelligence/machine learning (AI/ML)-driven solution developed by the Reserve Bank Innovation Hub (RBIH) to proactively identify mule accounts used for routing fraudulent proceeds.
As per RBI's press release dated 24 March 2026, the solution has already been operationalised across 26 banks and is being actively scaled. Early outcomes are encouraging, with the system detecting approximately 20,000 mule accounts per month in near real time, at a precision rate exceeding 90 per cent.[14] Initial pilot deployments, particularly in public sector banks, have demonstrated strong detection efficacy, underscoring the potential of AI-led interventions in strengthening the resilience of the financial ecosystem.

Organised cybercrime ecosystems

Cybercrime in India is increasingly organised. Enforcement actions have identified networks with explicit division of labour: technical specialists who build or rent attack infrastructure; recruiters who identify and manage money mules; money laundering specialists who move and layer funds; and logistics teams who convert and withdraw cash. India has its own organised cybercrime geography. Law enforcement operations have repeatedly identified fraud networks with explicit role specialisation — recruiters, script writers, mule account handlers, and fund dispersal teams — concentrated in areas including Jamtara (Jharkhand), Mewat (Haryana), and certain districts of Rajasthan and Uttar Pradesh.[15]

The internationalisation of cyber-enabled fraud is accelerating. Investigations and recovery increasingly involve cross-jurisdiction evidence and fund trails, where cooperation timelines often lag fraud velocity. As a result, faster coordination mechanisms, preservation triggers, and scalable digital evidence workflows become essential to improve attribution and recovery outcomes.

1.2 Digital crimes across sectors

BFSI and financial services

Banking, financial services, and insurance (BFSI) remain primary targets of cyber-enabled fraud because they combine high-value credentials, real-time payment rails, remote onboarding, and large transaction volumes. The investigative challenge in BFSI is rarely device-only; it requires correlating identity events (authentication, MFA, privilege changes), payment telemetry, beneficiary changes, customer communications, and third-party access into a defensible timeline. This is one reason national mechanisms for rapid reporting and fund-blocking are strategically important for limiting loss and improving recovery.

Insurance fraud in the digital crime category has evolved into a structurally different risk domain by 2026, characterised less by isolated false claims and more by organised, technology-enabled exploitation of underwriting, claims, and payment ecosystems. Fraud now spans digital identity misuse, data manipulation, and platform vulnerabilities rather than only post-event claims falsification. From a modus operandi perspective, the most material evolution is the convergence of cyber intrusion techniques with traditional insurance fraud. Industry and threat intelligence reports identify increasing use of AI-enabled artefacts significantly complicating evidentiary verification and increasing false-positive risk in automated claims environments. In parallel, systemic vulnerabilities—third-party access, digital onboarding, and real-time payment rails—are expanding attack surfaces, with fraud often executed as part of cross-institutional collusion or distributed low-value attacks designed to evade threshold-based detection systems

13 Man loses S$4.9 million in Strait of Hormuz funding assistance scam involving impersonation of PM Wong, Cabinet secretary, Channel NewsAsia, May 2026; Footage From Zoom Video Conference Involving Impersonation Of Senior Government Officials, Singapore Police Force, May 2026.
14 RBI's MuleHunter detects 20,000 mule accounts every month, The Financial Express, November 2025.
15 NCR belt emerges new cybercrime epicentre, Hindustan Times, May 2023; Joint team formed by Delhi Police to check cybercrimes from Mewat and Bharatpur, Hindustan Times, March 2023.

Fintech/Virtual digital assets

Virtual Digital Assets (VDAs) offer pseudonymity, borderless transfers, speed of settlement and limited centralised control that attract cybercriminal misuse. These features make VDAs particularly suitable for fraud proceeds routing, layering and obfuscation and cross-border laundering. Virtual Asset Service Providers (VASPs) form the operational backbone and act as entry/exit points (on-ramp/off-ramp) and transaction facilitators, thus categorised as high-risk nodes for financial crime monitoring.

This adoption has been accompanied by a corresponding rise in fraud typologies targeting retail participants, including manipulation through unregulated trading platforms, fraudulent investment schemes, compromised wallets and exchanges, and inducement-based NFT and token offerings. These vectors reflect the broader integration of VDAs into cyber-enabled financial crime ecosystems.

Indian retail investors have incurred losses via fraudulent crypto trading platforms, unlicensed digital lending apps, fake investment portals, hacking of wallets and exchanges, unhosted wallets and NFT-based 'rug pull' schemes. The Financial Intelligence Unit (FIU-IND) has mandated registration of Virtual Asset Service Providers (VASP) under PMLA since 2023, covering the compliant segment of crypto markets.

These risks are not limited to crypto ecosystems alone but extend across the broader fintech landscape, where digital payment platforms, lending applications, and online financial services have also been leveraged for fraud, impersonation, and mule account routing. However, unlike regulated fintech entities that operate within a well-defined compliance framework under RBI oversight and PMLA reporting obligations, the crypto ecosystem—while increasingly formalised through FIU IND supervision of VASPs—continues to exhibit residual exposure in decentralised exchange activities and peer-to-peer segments where regulatory visibility remains comparatively constrained. These areas, while evolving under regulatory oversight, illustrate the ongoing need to expand monitoring capabilities and strengthen cross jurisdictional coordination to ensure comprehensive coverage of emerging risk vectors.

Auto, Industrial Manufacturing and Energy

Fraud in manufacturing and energy takes several forms: vendor impersonation leading to payment redirection, manipulation of procurement systems, and insider-assisted theft of intellectual property. The energy sector faces additional exposure through operational technology (OT) environments where cyber intrusions can manipulate industrial control systems, a category of incident where the financial and physical consequences are difficult to separate. Several oil and gas sector incidents in India have involved ransomware deployed against both IT and OT networks simultaneously.

Government/Public digital infrastructure

India's digital public infrastructure — Aadhaar, UPI, DigiLocker, ONDC, and the Ayushman Bharat Digital Mission — processes vast quantities of sensitive personal and financial data. Documented misuse includes fraudulent Aadhaar updates used to redirect benefit payments, cloning of Jan Dhan account credentials, and phishing attacks targeting beneficiaries of government welfare schemes. CERT-In's latest advisories and vulnerability notes issued through 2026 reflect a rapidly evolving threat landscape impacting both government-facing and citizen-facing digital platforms. Recent alerts highlight sophisticated supply-chain compromise campaigns affecting widely used software components, as well as malware operations impersonating government services such as RTO and e-Challan platforms to target users. In parallel, CERT-In's April 2026 advisory underscores the emergence of AI-enabled cyber threats capable of automating vulnerability discovery, social engineering, and multi-stage attacks at scale.[16]

These developments build upon the high incident volumes recorded in 2025, where over 29 lakh cyber incidents were handled nationally, and collectively indicate a shift toward more automated, supply-chain-driven, and identity-centric attack patterns affecting critical digital ecosystems.[16]

E-commerce/Gig economy

The expansion of India's e-commerce and gig economy ecosystems has introduced new and evolving fraud vectors that reflect both scale and transactional velocity. Within e-commerce platforms, fraud manifestations include refund and return abuse, counterfeit or deceptive product listings, account takeover targeting stored value and loyalty instruments, and manipulation of seller reputation systems through coordinated activity.

[16] CERT-In: India's Frontline Defender against Cyber Threats, Press Information Bureau, Ministry of Electronics and Information Technology, January 2026, accessed 31 May 2026.

The gig economy further amplifies risk exposure due to its high-frequency, micro-transactional operating model. Platforms facilitating mobility, delivery, and freelance services process millions of low-value transactions daily, creating opportunities for fare manipulation, false service completion, synthetic activity generation, and coordinated rating or incentive abuse. These patterns increasingly resemble structured fraud operations rather
than isolated

1.3 Legal and regulatory framework

India's response to cyber-enabled financial crime is governed by a layered statutory architecture that has evolved rapidly since 2020. Understanding this framework is essential context for everything that follows — the investigative tools, the evidence standards, and the enforcement gaps all flow from what the law permits. The Information Technology Act, 2000 remains the core offence and incident-response backbone for many cyber offences and for CERT-In's powers, while the Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and Bharatiya Sakshya Adhiniyam, 2023 (BSA) modernise offence treatment, criminal procedure and evidentiary

handling. In parallel, **PMLA** is what chases the money, **DPDP** governs personal-data handling, and sectoral regulators such as **RBI, SEBI and IRDAI** impose operational controls on firms that sit inside the financial system or handle sensitive customer and market data. Prevention, reporting, evidence preservation, freezing/recovery, prosecution and restitution now sit across multiple legal instruments and regulators—not one statute.

What has materially improved for victims and investigators since 2024 is speed and digital processability. Together using I4C/NCRP/1930 for real-time complaint routing and fund-freezing support through CFCFRMS, and provisions like Zero e-FIR on NCRP, India is much better today at the 'first 24 hours' of a cyber-financial fraud than it was a few years ago. In terms of evidentiary readiness, BSA now expressly treats certain electronic and digital records as primary evidence and provides dedicated rules for the admissibility of electronic records, including a statutory certificate format. **BNSS** and the new criminal-law implementation stack also support electronic mode proceedings and technology-enabled evidence capture, with **e-Sakshya** positioned by the Government as a lawful, scientific and tamper-resistant digital-evidence mechanism. Accordingly, good cyber telemetry is no longer enough, it must become courtroom-capable evidence.

India cyber crime legal and risk architecture (2026)

Layered regulatory framework + fraud risk overlay

Law	Purpose	Associated risks
IT Act 2000	Core cybercrime offences	Phishing/account takeover; identity theft/fraud
BNSS 2023	Criminal procedure/update	Evidence challenges; digital forensic and admissibility issues
BSA 2023	Evidence admissibility	Evidence challenges; digital Forensic and admissibility issues
PMLA	Money trail tracing	Mule networks; crypto layering; transaction monitoring challenges
DPDP Act	Data protection overlay on investigations	Data access constraints; privacy vs investigation challenges
RBI/SEBI/IRDAI regulations	Sectoral anti-fraud controls	Sector-specific fraud control gaps; regulatory compliance and monitoring risks

Figure: Indian cyber crime and risk architecture

A May 2026 Supreme Court judgement clarifies that in addition to government-notified examiners under Section 79A IT Act, private experts with proven 'special skill and expertise in computer science and cyber-forensic' may certify digital evidence for admissibility (Part B of the Section 63(4) BSA certificate). This significantly reduces dependence on a very limited pool of official forensic labs, removing a major chokepoint that threatened to slow down corporate investigations and court cases.[17]

Where the law is strengthening is in end-state closure: cross-border reach, large-scale syndicates, and trial completion. That gap is especially visible in crypto, mule-account and offshore-platform cases. **PMLA** improves traceability and enforcement leverage, yet it does not eliminate jurisdictional friction, execution delays or recovery leakage once value has already moved through offshore rails or layered intermediaries.

On privacy and data handling, the **DPDP Act** regime matters more for internal investigations. It is not just fines or breach reporting—it is that fraud investigation, employee monitoring, insider-risk review, whistleblower triage and data sharing with law enforcement must all be designed with privacy governance in mind. DPDP is therefore an overlay on investigation practice; it does not replace criminal law, but it can constrain careless evidence collection or overbroad internal surveillance.

Sectoral rules are where prevention becomes operational reality. The frameworks and guidance issued by financial sector regulators on the subject show a more structured market-infrastructure style approach to stronger governance, response capability, threat intelligence, outsourced/cloud controls, cyber audit and recovery. For boards, this means liability increasingly flows from failures of governance and controls and not just from the original fraud event.

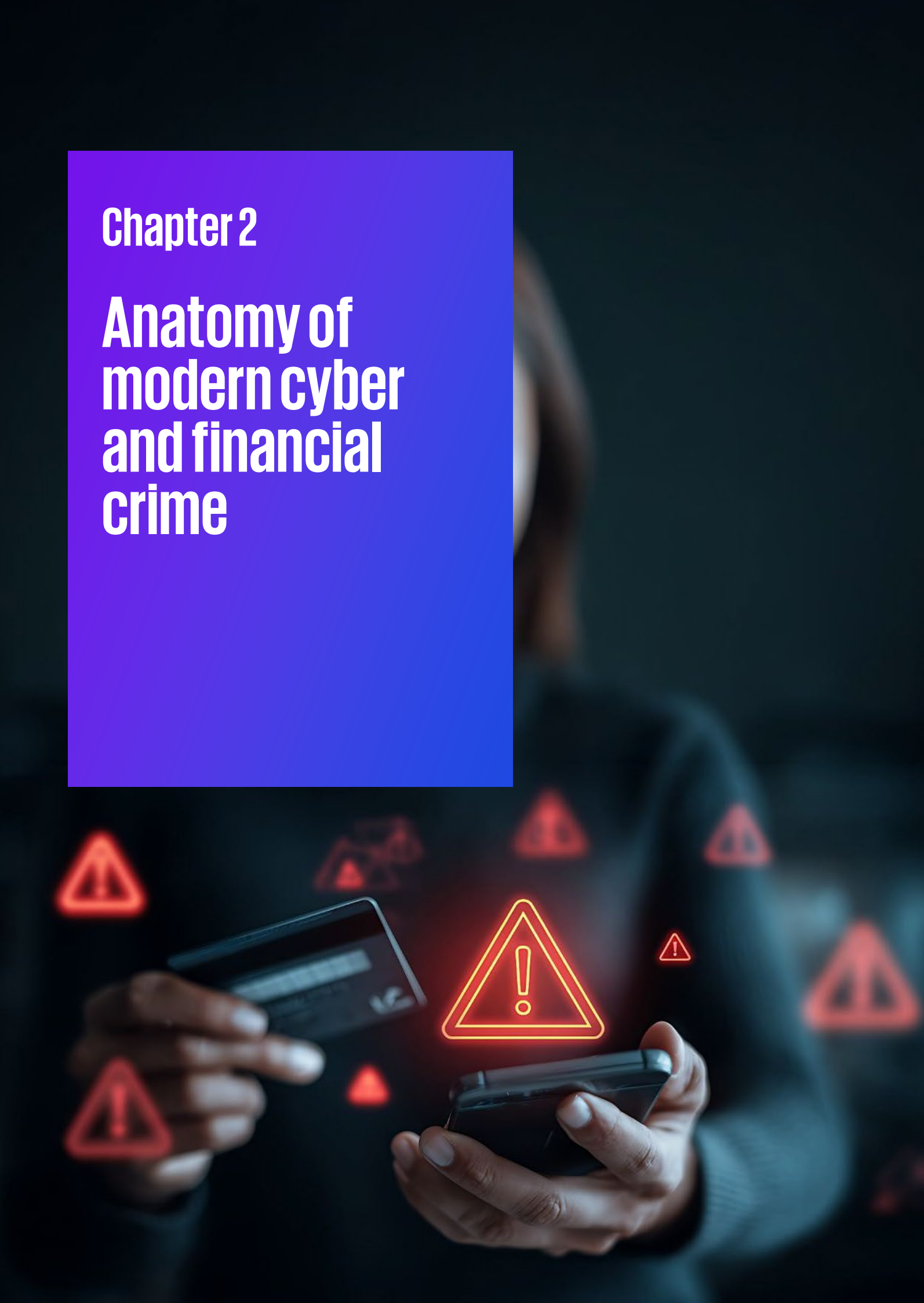
As depicted earlier, India has built a comprehensive, multi-layered legal system for cybercrime and financial fraud; however, it is also evident that risk does not disappear with regulation — it shifts to the edges of enforcement visibility.

International standards do not prosecute crime in India, but they increasingly shape what 'good enough' looks like. India's regulatory obligations at the international level flow from its **Financial Action Task Force (FATF)** membership which provides the AML/CFT benchmark and in 2026 explicitly highlighted cyber-enabled fraud as a major source of illicit proceeds globally. FATF's 2023 updated guidance on Virtual Assets and VASPs sets compliance expectations covering the travel rule, risk-based supervision of crypto exchanges, and reporting obligations for decentralised finance activities. **The Financial Stability Board's** 2023 recommendations on crypto-asset regulation — issued under a G20 mandate — complement FATF's framework and explicitly address DeFi and stablecoin risks. For Indian financial and cross-border firms, these frameworks matter because enforcement expectations, supervisory dialogues, partner-bank requirements and investor confidence are increasingly benchmarked against them—even when they are not directly binding statutes.

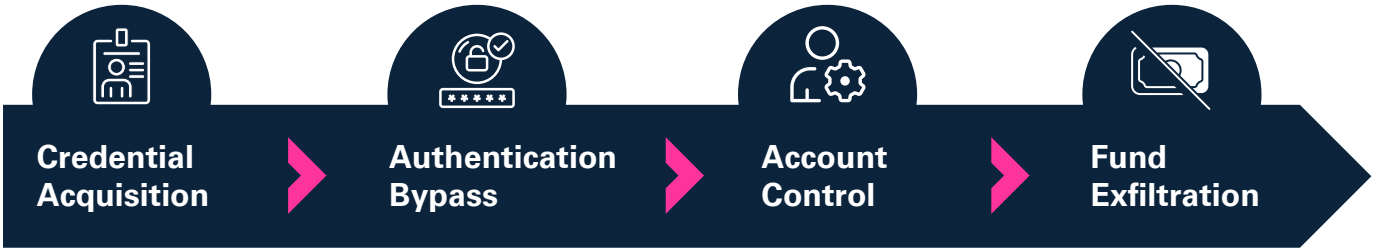
[17] Pune Bar Association v. Union of India and Others, Writ Petition (Civil) No. 599 of 2026, Supreme Court of India, May 2026.

Chapter 2

Anatomy of modern cyber and financial crime



2.1 Offender playbooks and attack vectors



Account takeover

Account takeover (ATO) is the foundational fraud technique from which most financial losses flow. The standard playbook runs in four stages: credential acquisition (through phishing, credential-stuffing against leaked databases, or malware); authentication bypass (SIM swap, OTP interception, or social engineering of bank call centres); action under account control (fund transfer, beneficiary addition, credit application); and exfiltration (movement of funds to mule accounts, often within minutes of takeover).

SIM swap fraud deserves particular attention. A fraudster who convinces a telecom provider to port a victim's number to a new SIM gains control of every OTP-based authentication linked to that number, banking, email, and payment apps simultaneously. Telecom providers have tightened SIM swap procedures following TRAI guidelines, but enforcement is uneven across operators and distribution channels.

Social engineering and deepfake fraud

Social engineering is the manipulation of human decision-making rather than technical systems. Its financial crime applications in India span a wide spectrum: vishing calls impersonating CBI or ED officers: messages on social media or instant messaging platforms from fraudulently cloned executive accounts; long-duration romance scams designed to extract investments into fraudulent platforms; and digital arrest scams.

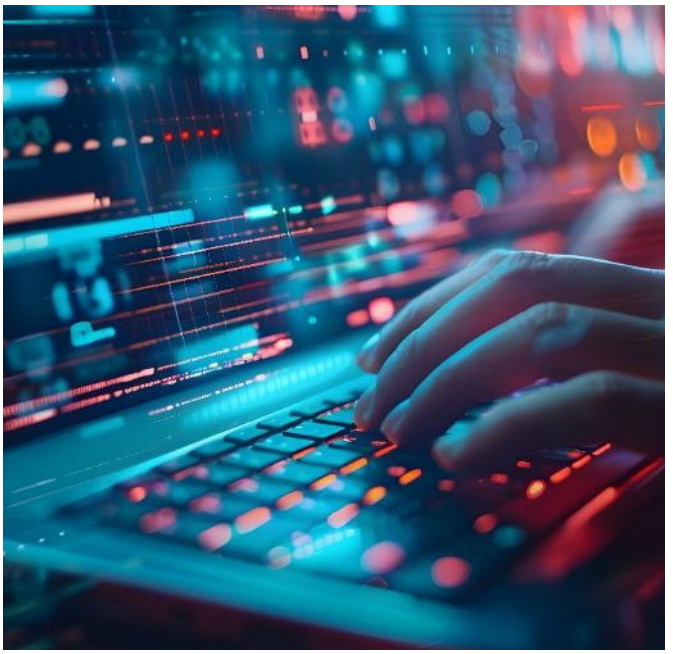
Digital arrest scams represent a distinct typology in India, where fraudsters posing as law enforcement officials coerce victims into remaining on continuous video calls for extended periods while transferring funds under the threat of fabricated criminal charges.

API/UPI/Payment misuse

India's payment infrastructure is API-first by design, which creates specific abuse surfaces. NPCI has documented cases of fraudulent UPI collect requests — legitimate-looking payment requests that a confused recipient approves, sending money to the fraudster rather than receiving it. QR code substitution at point-of-sale terminals redirects payments to fraudster accounts. While UPI is highly secure by design, some sophisticated frauds don't attack the user—they target the small weakness in underlying banking systems that process transactions. In simple terms, these attacks try to 'trick the banking system's timing, inputs, or login sessions' to behave incorrectly. For example, attackers may exploit timing gaps in how transactions are processed, alter transaction details before they are finalised, or hijack an active user session to complete unauthorised actions. These are not common vulnerabilities but have been observed in certain cases, and they underline the need for continuous strengthening of API security, transaction validation, and session controls across the ecosystem.

Insider and hybrid frauds

Insider-enabled and hybrid frauds (combining internal access with external networks) can be high-impact because they may bypass controls, manipulate workflows, and suppress early warnings. Investigation requires correlating privileged access events, approval workflows, transaction trails, and communications evidence to determine intent, method, and control failure points.



2.2 Evidence and discovery

Obfuscation techniques (VPN, TOR, Anonymisation)

Criminals have learned to operate within the architecture of privacy tools. VPN usage among cybercrime perpetrators is now standard practice; investigators requesting subscriber data from VPN providers frequently encounter no-logs policies, offshore incorporation, and non-cooperative jurisdictions. The TOR network routes traffic through multiple encrypted relays globally, making origin tracing dependent on operational security errors by the criminal rather than technical capability of the investigator. Residential proxy networks — in which compromised home routers are used as exit nodes — defeat IP-based attribution entirely.

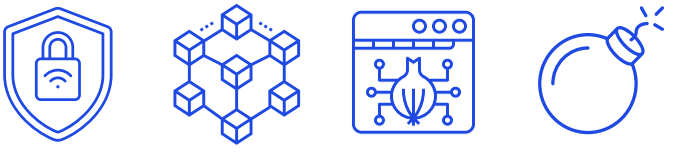
India's cyber investigation framework has steadily strengthened to keep pace with the growing sophistication of digital crime. The Information Technology Act provides a clear legal basis for lawful interception and monitoring, while regulatory measures led by CERT In, India's national cyber incident response agency, have significantly enhanced forensic readiness and traceability. Between 2022 and 2026, CERT In has adopted a more structured, enforcement led approach focused on data availability, rapid incident reporting, and attribution. Its directives mandating extended data logging, verified subscriber information for VPN services, and a six-hour incident reporting window have materially improved investigative responsiveness. Recent regulatory actions indicate increasing compliance maturity across service providers, supporting a transition toward a more accountable and auditable digital infrastructure aligned with cybercrime detection and investigation needs, even as international cooperation continues to evolve in a globally interconnected ecosystem.

Log tampering and artefact deletion

Sophisticated perpetrators often attempt to destroy or alter logs after gaining access to target systems. Common techniques include clearing event logs across operating systems, deleting command history, timestomping (altering file metadata to obscure access times), and disabling endpoint detection and response capabilities prior to executing fraudulent transactions. In cloud environments, attackers may delete certain specific sets of logs or disable container versioning. Detecting these anti-forensic actions is possible — the act of clearing logs often itself leaves a log entry — but only if the original event stream was being ingested by an independent SIEM platform that the attacker could not reach.

Crypto and layered financial flows

Cryptocurrency is the preferred layering instrument in large-scale cyber-financial crime. The standard pathway documented in Indian enforcement actions: proceeds from fraud are converted to USDT (Tether) via peer-to-peer exchanges or unlicensed VDAs; moved across multiple wallets using mixing services or privacy coins; converted back to fiat currency through exchanges in jurisdictions with limited KYC requirements; and finally moved into trade-based money laundering flows or hawala networks for final integration. The FATF has noted that the use of decentralised exchanges, which have no central operator to compel compliance, represents the current frontier of AML evasion.



FIU-IND has worked with Indian Virtual Asset Service Providers registered under PMLA to improve suspicious transaction reporting. In FY 2024–25, 47 entities were registered with FIU as reporting entities under the VASP category, but unregistered peer-to-peer activity remains largely opaque.[18]

[18] 49 cryptocurrency exchanges registered with FIU in 2024–25: Report, Press Trust of India, January 2026

DeFi, NFT, and cross-chain exploits

Decentralised Finance (DeFi) protocols — autonomous, smart-contract-governed financial services that operate without central administrators — create a specific enforcement problem. Unlike a licensed exchange, a DeFi protocol's governance is distributed across token holders, and the code itself executes transactions that no single party can reverse. When a DeFi protocol is exploited through flash loan attacks, oracle price manipulation, or reentrancy vulnerabilities in smart contract code, the attacker can drain protocol funds within a single blockchain transaction and immediately proceeds through automated mixing services or cross-chain bridges.

According to the WEF Global Cybersecurity Outlook Report 2026, cyber-attacks targeting exchanges, wallets and smart contracts have already caused multibillion dollar losses. In a major crypto-exchange breach in 2025 with losses exceeding USD1.5 billion, stolen funds were rapidly converted into assets difficult to trace or recover. Such fast pace of digital liquidity across multiple jurisdictions creates deeper risk for market confidence and liquid stability as per report. Cross-chain bridges, which allow assets to move between different blockchain networks, are a frequent attack vector; their complexity and the large asset pools they hold make them high-value, high-risk targets. In digital currency and crypto-related frauds, the critical evidence can be quickly fragmented, anonymised, or moved across jurisdictions. While transactions are recorded on blockchains, the link between a transaction and a real human identity is often weak or intentionally obscured, making certain types of evidence difficult to recover or act upon. Key evidences are difficult to trace include unhosted wallets, different blockchains, mixing services, DEX transactions, offshore or non-compliant platforms, etc. In digital currency fraud, the challenge is not the absence of data—but the absence of reliable identity linkage and control trails.[19]

Non-Fungible Token (NFT) fraud presents a different typology. The primary financial crime use cases have been wash trading — where an actor buys and sells NFTs between wallets they control, creating artificial price history for subsequent sales to genuine buyers at inflated prices — and using high-value NFT sales as a money laundering mechanism between criminal-linked wallets. In relation to fraud and market manipulation, it is observed that USD500 million was estimated to be lost to rug pull scams in 2025 alone. Typical NFT exploits include honeypots (trapping users into non-sellable tokens), hidden mint functions to inflate supply, fake ownership renunciations, hidden user balance modifiers and hidden fee modifiers,

For Indian investigators, DeFi and NFT fraud intersect with financial crime primarily at the exit point: domestic fraud proceeds entering the DeFi ecosystem for layering, and Indian investors victimised by NFT projects that were fraudulent from inception. There is no entity to compel — a DeFi protocol's on-chain code cannot be served with a production notice — and tracing through cross-chain bridges requires specialist analytics tools maintaining labelled address databases across multiple blockchain networks simultaneously. NFT-related fraud losses consistently remain in the hundreds of millions of dollars annually, with cumulative losses running into tens of billions when combined with broader crypto scams. While the scale of the NFT market has moderated from its peak, fraud activity continues to mirror wider crypto risk patterns—particularly phishing, identity manipulation, and rug pull schemes. Ultimately NFT fraud is less about 'digital art scams' and more about using NFTs as a gateway into larger financial fraud ecosystems involving identity compromise, wallet access, and asset laundering.

Anti-forensic tactics

Beyond log deletion, perpetrators use a range of techniques designed to frustrate forensic recovery. Full-disk encryption renders seized storage media inaccessible without keys. Self-destructing malware overwrites its own files upon detection. Steganography hides exfiltrated data inside image files transferred through otherwise benign channels. RAM-only malware leaves no persistent artefact on disk. Each of these techniques has a forensic counter, but executing the counter requires trained personnel, appropriate tools, and rapid deployment before the evidence is lost. In most Indian cases, there is a gap of 24-72 hours between incident detection and forensic deployment. In that window, volatile evidence is routinely lost.

[19] 2025 Crypto Crime Mid-Year Update: Stolen Funds Surge as DPRK Sets New Records, Chainalysis, July 2025; The Bybit Hack: Following North Korea's Largest Exploit, TRM Labs, February 2025.

Chapter 3

Digital evidence: From volatile to court-admissible

3.1 Nature of digital evidence

Volatility, fragmentation, cross-border issues

Digital evidence differs from physical evidence in three fundamental ways that courts and investigators must understand.

Volatility: RAM contents, network connections, and process tables exist only while a device is powered and changes constantly. Turning off a device to preserve it destroys this volatile layer entirely.

Fragmentation: A single financial transaction may leave artefacts across a mobile device, a banking server, a telecom record, a UPI switch log, and a beneficiary bank — each held by a different entity under different legal frameworks.

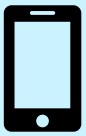
Cross-border: India's approach to cross-border evidence sharing is steadily becoming more agile as of 2026. While the formal channel of Mutual Legal Assistance Treaties remains essential, new parallel mechanisms and partnerships are injecting much-needed speed into the process. Indian agencies are increasingly leveraging rapid cooperation networks and exploring bilateral data-sharing agreements (such as potential CLOUD Act arrangements) to complement MLATs, enabling critical digital evidence can be preserved and accessed in time. Recent domestic legal advancements under the BNSS 2023 and DPDPA 2023 further streamline evidence handling on home ground, indicating an overall momentum toward a more responsive, globally coordinated framework for fraud investigations.

Structured vs. Unstructured Evidence

Structured digital evidence — database records, transaction logs, call detail records — can be searched, sorted, and queried systematically.
It is generally easier to authenticate and analyse. Unstructured evidence — email threads, instant messaging platform conversations, voice recordings, and social media posts — requires contextual analysis and is more susceptible to challenges of authenticity, completeness, and manipulation. Modern financial crime investigations generate both types in large volumes. The analytical challenge is integrating these streams into a meaningful narrative that a court can follow.

AI-generated content introduces a third category: evidence that may be authentic, synthetic, or deliberately manipulated in ways that are not apparent to visual inspection. Courts will increasingly face questions about the provenance of audio recordings, video footage, and even chat transcripts that could have been generated or altered using AI tools. The appropriate forensic response is not to reject AI-adjacent evidence wholesale, but to require provenance verification — analysis of metadata, compression signatures, and generation artefacts — before placing weight on it.

3.2 Evidence sources across crime types

Evidence Source	Significance	Challenges
Mobile Devices (Smartphones/Tablets) 	• Primary 'command and control' device for fraud actors (OTP interception, mule coordination, phishing execution) • Forensic artefacts: chats, app data, call logs, browser history, GPS trails • App-level intelligence (banking, UPI apps, crypto wallets) provides transaction trails	• Strong encryption and secure enclaves limit physical extraction • Volatile artefacts (deleted chats, ephemeral messaging) • Dependency on advanced forensic tools and lawful access mechanisms
IoT/Smart Devices (CCTV, Wearables, Smart speakers, Connected vehicles) 	• Provides contextual and corroborative evidence (presence, movement, behavioural patterns) • Can validate timelines (e.g., CCTV logs, smart lock entries, wearable activity) • Captures environmental and biometric data (audio snippets, motion logs)	• Device heterogeneity—no standardised data formats or tools • Limited storage leads to rapid overwriting of evidence • Data distributed across device + cloud + third-party services • Jurisdictional and encryption barriers
Cloud/SaaS Platforms (Email, CRM, Collaboration tools) 	• Core repository of enterprise fraud evidence (emails, file sharing, audit logs, identity logs) • Metadata (access logs, IP addresses, modification trails) provides **intent and timeline reconstruction** • Central in BEC, insider fraud, ransomware investigations	• Data spread across multiple jurisdictions ('crime scene has no location') • Short log retention windows (often ~30–90 days unless preserved) • Multitenancy restricts physical imaging; reliance on API/logical extraction • Legal dependency on service providers for access
Payment Ecosystems (Banking Systems, UPI, Wallets, Card Networks, NPCI) 	• End-to-end financial trail across payer bank, intermediary switch, beneficiary bank • High granularity: timestamps, device IDs, IP addresses, VPA/account linkages • Enables fund flow reconstruction and mule network mapping	• Fragmented data ownership across banks, NPCI, wallets leads to coordination complexity • Time-sensitive freezing requirements (fraud proceeds move rapidly) • Data access governed by regulatory approvals and inter-bank cooperation
Telecom Metadata (CDR, IPDR, EDR, Subscriber Logs) 	• Critical for link analysis (who spoke to whom, when, and from where) • Establishes communication patterns, network mapping, and attribution • IPDR enables correlation with internet sessions, portals, platforms and app usage • Retained for minimum two years (India regulatory mandate)	• Requires lawful interception/LEA coordination • Increasing usage of VoIP/OTT apps reduces visibility in traditional telecom logs • Content not available—only metadata (requires corroboration)

Evidence Source	Significance	Challenges
Endpoint Systems (Laptops/Desktops/ Servers) 	• Full-spectrum artefacts (emails, documents, browser artefacts, malware traces) • Critical for insider fraud, ransomware entry vectors, phishing execution • Provides persistence indicators and attack tooling evidence	• Anti-forensic (log wiping, encryption, disk tampering) • Large data volumes leads to time-intensive imaging and analysis • Endpoint may not contain cloud-native activity (shift to SaaS)
Network Logs/Security Infrastructure (Firewall, Proxy, SIEM, EDR) 	• Provides attack path reconstruction (lateral movement, exfiltration, C2 communication) • Correlates multi-system events for attribution • Vital in enterprise cyber incidents and APT investigations	• Log retention limitations (often 30–180 days) • Noise vs signal problem (high volume, low signal ratio) • Misconfigured logging may lead to evidentiary gaps
Dark Web/Open-Source Intelligence (OSINT) 	• Links fraud infrastructure to threat actors (forums, leaked databases, credential dumps) • Provides attribution leads and modus operandi insights	• Attribution uncertainty (alias-based ecosystems) • Legal admissibility concerns • Requires specialised monitoring tools and intelligence capabilities

Devices (Mobile, endpoint, IoT)

Mobile devices are the most forensically significant evidence source in most Indian cybercrime cases. A suspect's smartphone may contain the complete operational record of a fraud: social media or instant messaging platforms used to coordinate attacks, payment applications used to transfer proceeds, call logs showing communication with victims, photos of fraudulent documents, and location data placing the suspect in relevant locations. Forensic extraction from modern devices requires specialised digital forensic tools widely used by investigative agencies and the choice of extraction method (logical, filesystem, physical, or chip-off) affects what is recoverable and what is admissible.

IoT devices — smart speakers, connected cameras, wearables — are an emerging evidence source. A smart speaker's interaction log may corroborate or contradict an alibi. A connected CCTV camera may provide location evidence. These sources are largely unexplored in Indian criminal investigations, partly because there is no standardised procedure for their forensic acquisition.

Cloud and SaaS environments

Cloud evidence presents the most significant operational challenge in modern digital investigations. Evidence may be stored in public cloud data centres outside or locally within India. Data retention policies may result in automatic deletion within 30-90 days of an event — a window that often expires before a formal evidence preservation request reaches the provider. SaaS applications present additional complexity: the application operator may not retain the underlying data that a financial crime investigation requires or may have deleted it pursuant to their own retention schedule. Data centers sometimes don't consider forensic readiness as an important business concern itself.

The CERT-In direction of April 2022 requires organisations to retain logs for 180 days, improving this situation for regulated entities, though compliance monitoring remains incomplete. Ephemeral machine and storage are another concern when it is not storing persistent logs after an incident needs investigation.[20]

[20] Directions under Section 70B(6) 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, April 2022.

Payment ecosystems

The Indian payment ecosystem is among the most forensically rich in the world. UPI mandates logging at multiple points: the remitter's payment app, the remitter's bank (NPCI designated Payer PSP), the NPCI switch itself, the beneficiary PSP, and the beneficiary bank. Each log is maintained with transaction ID, timestamp, device binding data, and — for many transactions — the Aadhaar-linked beneficiary details. In FY 2025-26, UPI processed 241 billion transactions worth approximately INR314.23 lakh crore, generating an enormous forensic audit trail when properly accessed. In practice, accessing data from multiple regulated entities under different regulatory umbrellas requires coordinated legal orders that few investigators know how to obtain simultaneously.[21]

Telecom/metadata

Call Detail Records (CDRs) and Internet Protocol Detail Records (IPDRs) from telecom operators are among the most consistently valuable evidence sources in Indian cybercrime investigations. A CDR traces the time, duration, and cell tower location of calls made from SIM. Tower dump analysis — requesting records of all devices connected to a specific cell tower during a defined time window and IPDR provides internet usage metadata: IP address, login/logout timestamps, session info — have produced breakthroughs in multiple high-profile cyber fraud cases. Telecom operators (under Unified License/UASL) must retain CDR, TDR/EDR, and IPDR records for a minimum of two years. The legal authority requests this data exists under Section 94 of the Bharatiya Nagarik Suraksha Sanhita 2023. Data access is governed under Telecommunications Act/IT Act + DoT license conditions, Section 94 BNSS and Telecom Act 2023. India's telecom data retention framework is relatively robust for metadata-driven investigations, but its effectiveness is increasingly constrained by the shift toward encrypted, platform-based OTT communication and cross-border data flows.

[21] UPI completes 10 glorious years, emerges as world's largest real-time payments platform, anchoring India's digital economy, Press Information Bureau, Government of India, April 2026.

3.3 Evidence lifecycle

Identification

Identifying what evidence exists and where it resides is one of the first and often one of the most time-sensitive phase. First responders must resist the instinct to examine devices immediately — uncontrolled access to a live device can overwrite the data they are trying to preserve. A systematic identification process maps the evidence landscape: which devices were involved, which accounts, which cloud services, which network infrastructure, and which third-party platforms hold potentially relevant data. This mapping must happen quickly because many evidence sources are time limited.

Collection

Collection must follow documented procedures to withstand legal scrutiny. For physical devices, this means photographing the scene, recording device state (on/off, battery level, network connectivity), and using Faraday shielding to prevent remote wipe commands from reaching the device before forensic extraction. For cloud and SaaS evidence, collection means issuing formal preservation requests to platform operators and, where possible, performing collection through forensically validated tools that produce verifiable output. Chain-of-custody documentation begins at collection and must be maintained continuously.

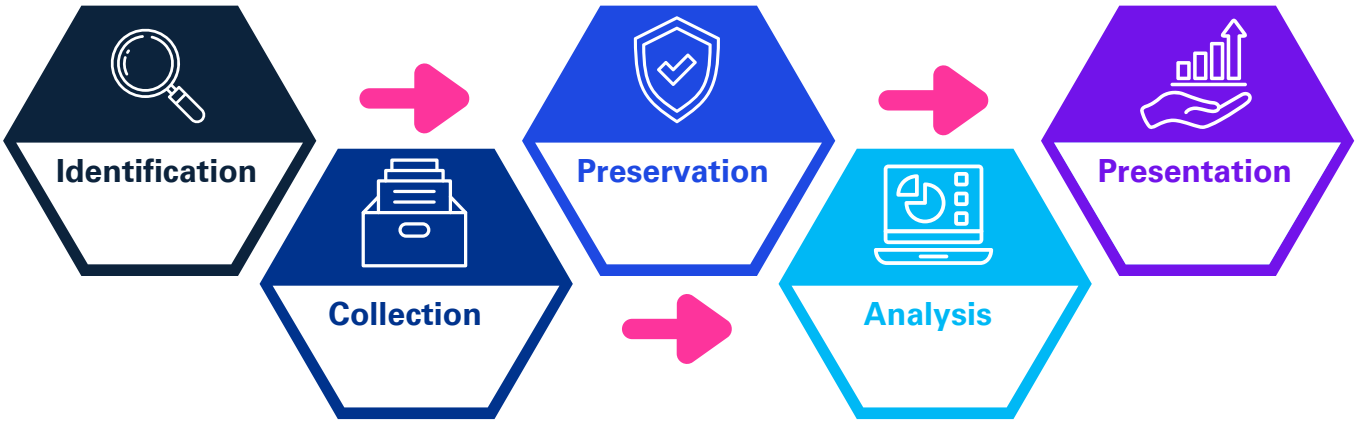
Preservation

Preservation creates a forensic copy — typically a bit-for-bit image of storage media verified by cryptographic hash — that protects the original from alteration while enabling examination of the copy. The hash value (SHA-256 is the current standard) serves as a tamper-evident seal: any subsequent modification to the image will produce a different hash, which is immediately detectable. Under Section 63 of the Bharatiya Sakshya Adhiniyam 2023, electronic evidence must be accompanied by a certificate attesting to the process of production, identity, and absence of tampering. Forensic imaging that generates hash-verified copies satisfies this requirement. Casual screenshots or forwards on instant messaging platforms do not.

Analysis and presentation

Forensic analysis transforms raw evidence into findings that an investigator, prosecutor, and ultimately a court can understand. This requires both technical and communication skills that are rarely combined in one individual. The technical analyst must recover deleted files, reconstruct timelines from fragmented log data, correlate device artefacts with network activity and identify indicators of anti-forensic tampering. The presenting expert must translate these findings into testimony that survives cross-examination by a technically versed defence advocate.

Courts have repeatedly criticised forensic reports for being too technical for judicial comprehension or too superficial to withstand scrutiny. The ideal forensic report includes: a plain-language summary of findings; a methodology section describing every tool used with version numbers and settings; a chain-of-custody appendix; hash verification records; and annotated exhibits. In fraud cases, a timeline of digital events correlated with the alleged financial transactions is often the most persuasive presentation format.



Chapter 4

Advanced forensic capabilities

4.1 Cloud native forensic

Multi-cloud investigations

Many large Indian enterprises now operate across multiple cloud providers — typically a primary provider supplemented by secondary platforms for specific workloads. A fraud investigation that touches enterprise infrastructure may need to collect evidence from multiple cloud systems simultaneously, each with different data structures, log formats, API access mechanisms, and legal data request processes. The investigator must map which workloads run where, understand each provider's logging architecture, and determine what is retained by default versus what requires explicit configuration.

For instance, while cloud environments typically record administrative or control plane activities by default, detailed data access events—such as who accessed specific files or datasets—often require explicit configuration. In the absence of such enhanced logging, organisations may be unable to conclusively determine whether how and by whom sensitive data was accessed or exfiltrated, even where a broader security incident has been confirmed.

Regulatory interventions, including the CERT-In directions issued in April 2022 mandating a minimum log retention period of 180 days, have addressed this gap by improving the availability of forensic data for regulated entities. However, the effectiveness of these measures continues to depend significantly on proactive enablement of granular logging controls at the platform level.[22]

SaaS evidence recovery challenges

Software-as-a-Service applications — collaboration tools, CRM platforms, HR systems — are increasingly central to how organisations operate and communicate. They are also forensically opaque. Unlike a physical server that an investigator can image, a SaaS application presents its data through an API or an administrator console that the forensic investigator cannot fully control. Export capabilities vary: some platforms export comprehensive, time-stamped data; others produce limited exports that miss metadata, edit histories, or deleted content.

The evidentiary value of SaaS data — particularly in insider fraud and intellectual property theft cases — can be substantial. A collaboration platform's message history may show a disgruntled employee systematically downloading sensitive customer data in the weeks before departure. Recovering and authenticating this evidence requires a forensic methodology specific to each platform and a clear legal authority to request platform-side data from the provider.

Identity-centric investigations

Cloud-native environments shift the forensic focus from devices to identities. In a traditional investigation, a device is the primary evidence artefact. In a cloud environment, an identity — a username, an API key, a service account — is the actor that leaves artefacts in logs. Compromised identities are used to access cloud resources without any malware being deployed on a physical device. Investigating a cloud-based fraud therefore requires reconstructing the identity's activity: when it authenticated, from where, which resources it accessed, and whether its permissions were escalated at any point.

Identity and Access Management (IAM) logs are the primary evidence source for this analysis. They must be correlated with application logs, network flow data, and — where available — endpoint detection data. This correlation requires tooling (a security monitoring platform or a cloud security posture management platform) and analytical skill that few Indian organisations currently have in-house.

[22] Directions under Section 70B(6) 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, April 2022.

4.2 AI in forensic investigations

Pattern recognition and anomaly detection

Machine learning models applied to financial transaction data can detect fraud patterns that rule-based systems miss. Supervised models trained on labelled fraud cases identify known typologies — rapid sequential withdrawals from multiple ATMs, unusual merchant category codes, atypical geolocation sequences. Unsupervised models identify anomalies relative to an individual's transaction history without requiring labelled training data, which is valuable for detecting novel fraud patterns.

> The RBI's MuleHunter.AI initiative, developed at the Reserve Bank Innovation Hub and referenced in the RBI Annual Report 2024-25, is a domestic example of deploying AI specifically to identify mule accounts used in routing fraudulent proceeds.

Several Indian public sector banks have deployed AI-based transaction monitoring in collaboration with technology vendors.

NLP for fraud detection

Natural Language Processing (NLP) is applied in financial crime investigation at several points: screening loan applications for textual inconsistencies that suggest fabrication; analysing financial statement narratives for language patterns associated with earnings management; monitoring internal communications for terms associated with fraud risk; and — in law enforcement use cases — processing seized devices to identify relevant communications from large data sets.

India's linguistic diversity creates both a challenge and an opportunity. Fraudulent communications routinely occur in multiple languages like Bengali, Hindi, Marathi, Tamil, and other regional languages, often mixed with English. NLP models trained primarily on English text perform poorly on code-mixed text, which is the dominant register of informal digital communication in India. Building or fine-tuning models for Indian language fraud detection is a research priority that has received insufficient attention.

Deepfake detection

For forensic use, deepfake detection findings must be presented with appropriate epistemic caution: current models can raise or lower the probability of synthetic generation but cannot definitively prove it in all cases. Courts should be cautioned against treating detection model outputs as binary proof. The correct approach is to present the detection analysis as one element of a broader evidence picture, alongside metadata analysis, source authentication, and expert comparison with confirmed authentic recordings.

Post-Quantum Cryptography — Planning for the next Frontier

Current public-key cryptographic standards — RSA, ECC, and the Diffie-Hellman protocols that underpin TLS, blockchain infrastructure, and most financial systems — rely on the computational difficulty of factoring large integers or solving discrete logarithm problems. Quantum computers operating on Shor's algorithm could theoretically solve these problems efficiently. A cryptographically relevant quantum computer does not exist as of 2025, but the development trajectory means that financial institutions, regulatory bodies, and forensic infrastructure managers should begin transition planning now rather than wait for the threat to materialise.

For forensic practice, the implications are threefold. Evidence encrypted with current algorithms and challenged in court years from now may face questions about integrity if those algorithms have been broken — a risk that remains theoretical for the near term but is worth acknowledging. Blockchain evidence collected now may face authentication challenges in a post-quantum world if the wallet signatures used to establish ownership become computationally forgeable. Communication interception capabilities in financial crime investigation depend on TLS-protected channels; PQC migration changes the decryption landscape for future evidence collection.

Indian financial institutions and forensic investigation agencies must now proactively align with evolving Post-Quantum Cryptography (PQC) standards, particularly those issued by NIST, and initiate structured cryptographic asset discovery and inventory exercises. This includes systematically identifying dependencies on quantum-vulnerable algorithms such as RSA and ECC across critical systems, even where full-scale migration may be phased over the next few years. There is a strong case to establish a formal 'crypto-agility' roadmap integrating PQC readiness into enterprise risk management, vendor governance and technology modernisation programs for organisations.

India's regulatory stance on PQC has materially evolved in 2026. The Reserve Bank of India has constituted an expert committee under the Quantum Secure and Adaptive Financial Ecosystem (Q-SAFE) initiative to assess sectoral cryptographic exposure, mandate Cryptography Bills of Materials (CBOMs), and recommend a transition roadmap for quantum resilience. In parallel, national efforts under the Quantum Safe Ecosystem Task Force and the National Quantum Mission are formalising phased migration frameworks and testing ecosystems for quantum-safe adoption.[23]

In this context, organisations should treat PQC readiness not as a distant transformation but as an immediate risk-management and crypto-agility objective, aligning inventory, risk classification, and pilot migrations with global timelines that anticipate the gradual retirement of legacy public-key cryptography over the next decade.

4.3 Automation and forensic labs of the future

Digital forensic labs

India's forensic modernisation drive has given national labs cutting-edge digital capabilities, but a gap remains at many state labs that are still improving their technology and skills. This is a natural challenge as digital crime grows – state-level teams handle most cases but have historically relied on central labs for advanced support. The path forward is to democratise forensic capacity by ensuring every region has core capabilities: up-to-date forensic tools, secure data extraction and analysis environments, rigorous evidence procedures, and trained analysts.

A functioning digital forensic lab requires, at minimum: workflow management system, licensed IT assets and advanced forensic extraction tools; secure high bandwidth connectivity between labs, WORM storage, write-blockers; a clean, air-gapped analysis environment; chain-of-custody logging; ticketing and troubleshooting management system; and trained staff and analysts who are current on tool capabilities.

A national capacity review and uplift programme could harmonise these elements, leading to a stronger, more evenly equipped forensic network that benefits the entire investigative ecosystem.

Automation pipelines

Automated Forensic pipelines — systems that ingest raw evidence artefacts, unstructured data and information, parse them according to defined taxonomies, correlate them across sources, and produce structured outputs for human review are in operational use at the most advanced investigative agencies globally. In India, automated pipelines are used by central agencies for CDR/IPDR analysis and transaction tracing, but the technology is not standardised or available at every state level.

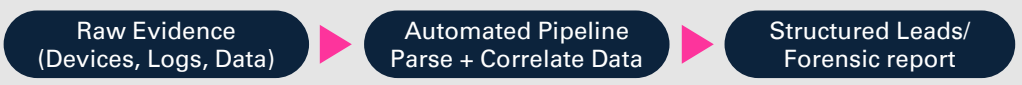
The potential of automation is not to replace forensic analysts but to handle volume. Modern investigations routinely involve data on the order of tens to hundreds of gigabytes per device, hundreds of thousands of telecom records, and months (or longer) of financial transactions history related to hundreds of accounts—quantitites far too much for manual review in investigation timelines. Automated initial triage enables analysts to focus effort where it matters.

Evidence Management Systems

A Digital Evidence Management System (DEMS) or Case Management System (CMS) tracks every item of evidence from collection through analysis to court production: who had custody, when, what actions were performed, and what the hash values are at each stage. Without a DEMS, chain-of-custody integrity depends on paper records that are difficult to audit and easy to challenge.

Several commercial DEMS/CMS products are available and in use at Indian central agencies. The challenge is extending this to state police and to the private sector. Corporate fraud investigations that are later referred to law enforcement frequently suffer from inadequate evidence management in the initial corporate investigation phase — evidence has been handled, analysed, and shared without documentation, making it difficult to authenticate before a court. Private sector forensic practitioners should adopt DEMS/CMS tools as standard practice, not optional good practice.

Automated forensic pipeline



Digital Evidence Management Workflow (DEMS)

[23] Quantum Secure and Adaptive Financial Ecosystem (Q-SAFE) – Setting up of an Expert Committee, Reserve Bank of India, May 2026.

Chapter 5

Financial fraud and money trail investigation

5.1 Typologies of financial fraud

Fraud typology	Key characteristics	Core challenges
Real-time payment frauds (UPI/instant payments) 	• Exploit instant settlement ecosystems (UPI, IMPS) • Social engineering-led: phishing, remote access, QR scams • Dual modes: demand-side (victim inducement) and supply-side (account compromise) • Operate at scale leveraging telecom + mule accounts.	• Narrow 'golden hour' for recovery due to immediate fund movement • Fragmented response across banks, fintechs, telecom • Traceability diluted via mule accounts and rapid layering • Heavy dependence on customer awareness vs system controls.
Trade-Based Money Laundering (TBML) 	• Misuse of trade flows: over/under invoicing, false documentation • Uses legitimate trade ecosystem to disguise illicit flows • Strong cross-border component with multi-jurisdiction participants • Integrated into broader AML layering techniques.	• Document-heavy, low visibility transactions (invoices vs actual goods) • Difficult to validate price/quantity authenticity across jurisdictions • Dependency on banks as primary detection gatekeepers • Regulatory coordination gaps across customs, banks, regulators.
Insurance and claims fraud 	• Dual-layer typology: - Opportunistic: inflated claims, misrepresentation - Organised: collusion (hospitals, agents, intermediaries) • Increasing cyber-enabled fraud vectors (fake portals, impersonation) • Industry-wide categorisation across internal, claims, external frauds.	• Highly distributed fraud ecosystem across value chain • Collusion networks difficult to detect without shared data • Shift from reactive to governance-led detection frameworks • Need for centralised intelligence sharing (IIB integration).
DeFi/NFT/ Emerging Platform Fraud 	• Includes rug pulls (exit scams) and wash trading (market manipulation) • Blockchain-driven transactions with pseudonymous actors • On-chain transparency but weak off-chain identity linkage • Manipulation of liquidity pools and artificial volume creation.	• Attribution gap – wallet ≠ real identity • Rapid emergence of new tokens/projects (high velocity risk) • Jurisdictional regulatory arbitrage (global, decentralised platforms) • Requires advanced blockchain analytics + OSINT correlation.

Fraud Typology	Key Characteristics	Core Challenges
Corporate Fraud (Enterprise-Level) 	• Multi-dimensional: loan fraud, procurement fraud, shell entities, financial misstatements • Often involves insider collusion + external syndicates • Increasing tech-enabled fraud (ERP manipulation, deepfake approvals) • Embedded within legitimate business processes.	• Complex evidentiary trail across systems (ERP, email, banking) • High legal/regulatory scrutiny (SFIO/ED type interventions) • Insider involvement complicates detection and whistleblowing • Requires integrated forensic approach (financial + digital + behavioural).

Fraud is no longer a transaction-level anomaly—it is an ecosystem-level risk driven by speed, anonymity, and cross-border complexity. Each typology demands a different control philosophy: real-time disruption (UPI), document intelligence (TBML), network analytics (Insurance/Corporate), and blockchain attribution (DeFi).

UPI/Real-Time Payment Frauds

UPI's real-time settlement architecture eliminates the settlement window that traditional fraud controls relied on. Once a transaction is authorised, funds reach the beneficiary within seconds. Reversals require cooperation from the beneficiary bank — cooperation that is frequently not forthcoming when the account is a mule operated by parties who deny knowledge or cannot be traced.

UPI fraud typologies break into two categories. Demand-side frauds manipulate the victim into approving a payment: fraudulent collect requests, QR code substitution, and social engineering that confuses the direction of a transaction. Supply-side frauds compromise the underlying account through credential theft, SIM swap, or application exploitation.

Real-time payment systems compress the recovery window. In a high-frequency environment, the practical determinant of recoverability is how quickly a victim reports and how quickly institutions can trace and freeze onward hops through mule chains. For 2025, MHA reporting through NCRP records 24,02,579 online financial fraud complaints with INR22,495 crore reported loss; the CFCFRMS mechanism reported saving more than INR8,189 crore up to 31 December 2025. These figures underscore why rapid reporting, coordinated response, and evidence readiness are central to next-generation forensic in payments.[24]

UPI scale continued to expand in FY 2025–26, with government reporting noting over 24,162 crore annual transactions valued at approximately INR314 lakh crore. At this magnitude, investigators must treat payments evidence as distributed across multiple custodians (payer PSP, NPCI switch, payee PSP, beneficiary bank) and design evidence collection pathways that can be activated quickly.[25]

[24] Cybercrime Reporting and Investigation, Press Information Bureau, Ministry of Home Affairs, February 2026; Rajya Sabha Unstarred Question No. 1341, Ministry of Home Affairs, February 2026.
[25] UPI completes 10 glorious years, emerges as world's largest real-time payments platform, anchoring India's digital economy, Press Information Bureau, Government of India, April 2026.

Trade-Based Money Laundering

Trade-based money laundering exploits the complexity and document intensity of international trade to move and integrate criminal proceeds. The basic mechanisms — over-invoicing, under-invoicing, multiple invoicing for a single shipment, and falsely described goods — have existed for decades. What has changed is the increasing use of digital trade documentation, which reduces the friction of creating falsified records and allows fraud operations to scale without proportionally larger teams.

India's Directorate of Revenue Intelligence and the Enforcement Directorate have pursued TBML investigations across sectors including diamonds,

chemicals, and textiles — areas with significant export volumes where price benchmarking across jurisdictions is inherently difficult. FATF guidance on TBML identifies the financial institution's role as critical because letters of credit and trade finance instruments pass through banks that have visibility into transactions that customs authorities may not. Indian banks have improved TBML alert programmes following RBI guidance, but the trade finance analyst skill set remains scarce in most compliance teams.

Insurance and Claims Fraud

Insurance fraud in India operates at two levels simultaneously. At the retail level, individual policyholders inflate or fabricate claims — a motor accident pre-staged, a hospitalisation extended beyond clinical necessity, a life policy taken on a terminally ill person without disclosure. At the organised level, fraud rings coordinate across multiple participants: hospitals that certify fictitious procedures, intermediaries who recruit policyholders, and insiders at insurance companies who suppress verification checks.

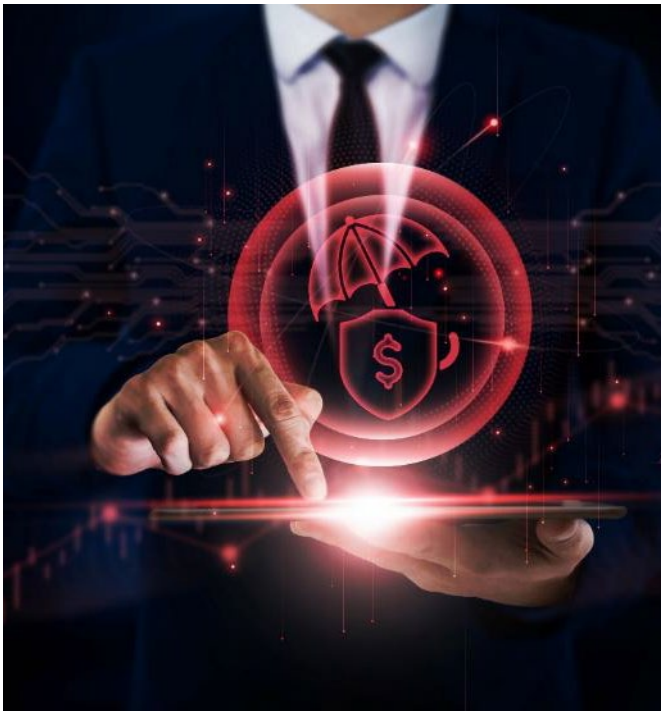
IRDAI's Insurance Fraud Monitoring Framework Guidelines 2025, effective April 2026, require insurers to implement fraud management systems with defined data-sharing obligations through the Insurance Information Bureau (IIB). The IIB's pooled claims database has already identified fraud clustering around specific hospital networks and geographic clusters — a pattern that no individual insurer's internal data would reveal because the fraud is deliberately distributed to stay below each institution's individual alert thresholds.[26]

DeFi, NFT, and Emerging Platform Fraud

Beyond conventional financial crime, decentralised platforms have opened new fraud typologies that Indian regulators and investigators are only beginning to engage with. DeFi investment scams follow a consistent playbook: a platform offers implausibly high returns on liquidity provision or yield farming; early investors receive returns funded by later entrants; the operators eventually drain pooled funds in what the crypto industry terms a rug pull. Unlike a conventional Ponzi scheme, the smart contract architecture provides a veneer of technical legitimacy — the code executes as written, even when the design is inherently extractive.

NFT fraud exploits the absence of intrinsic value benchmarks. A fraudster can create and sell NFTs at artificially inflated prices through wash trading, establishing a fictitious transaction history that makes subsequent sales to genuine buyers appear supported by market evidence. The proceeds are then layerable through further NFT transactions before conversion to fiat.

For investigators, the key evidence in DeFi and NFT fraud cases lies on the public blockchain: the transaction ledger is transparent, permanent, and globally accessible. The investigative challenge is attribution — connecting blockchain wallet addresses to real-world identities. This requires blockchain analytics tools, enhanced due diligence, KYT mechanisms, cooperation from exchanges where funds were ultimately cashed out, and PMLA-backed jurisdiction over registered VASPs. Enforcement actions demonstrate that this chain of attribution is achievable for the domestic segment of the fraud — but breaks down at the cross-border layer where unregistered exchanges and privacy coins are used.



[26] Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025, Insurance Regulatory and Development Authority of India, October 2025.

Corporate fraud

Corporate fraud in India encompasses a wide spectrum: loan fraud through falsified financial statements and collateral documentation; procurement fraud through bid-rigging and vendor impersonation; asset misappropriation by employees; and financial statement manipulation to meet market expectations or debt covenant thresholds. These categories overlap in many large cases. High-value banking frauds typically combine falsified financials at the borrower level, weak due diligence at the bank level, and active suppression of early warning signals by insiders at one or both institutions.

The Serious Fraud Investigation Office has investigated over a thousand cases since its establishment, with the proportion involving technology-enabled fraud rising each year.[27] Common patterns include the use of multiple shell companies to create circular transactions that inflate revenue, transfer funds to promoter-linked entities, cooking the balance sheets or obscure the trail of diverted loan proceeds.

RBI's 2024 Master Directions on Fraud Risk Management impose specific obligations around Early Warning Signals (EWS) — financial indicators that should flag loan fraud risk before it crystalises into an unrecoverable loss. In practice, the gap between an EWS trigger and a fraud classification has been a persistent enforcement challenge. Banks with governance weaknesses have either suppressed or delayed EWS reporting, allowing fraud to grow to sizes that exceed recovery prospects before regulators or boards are formally notified.[28]

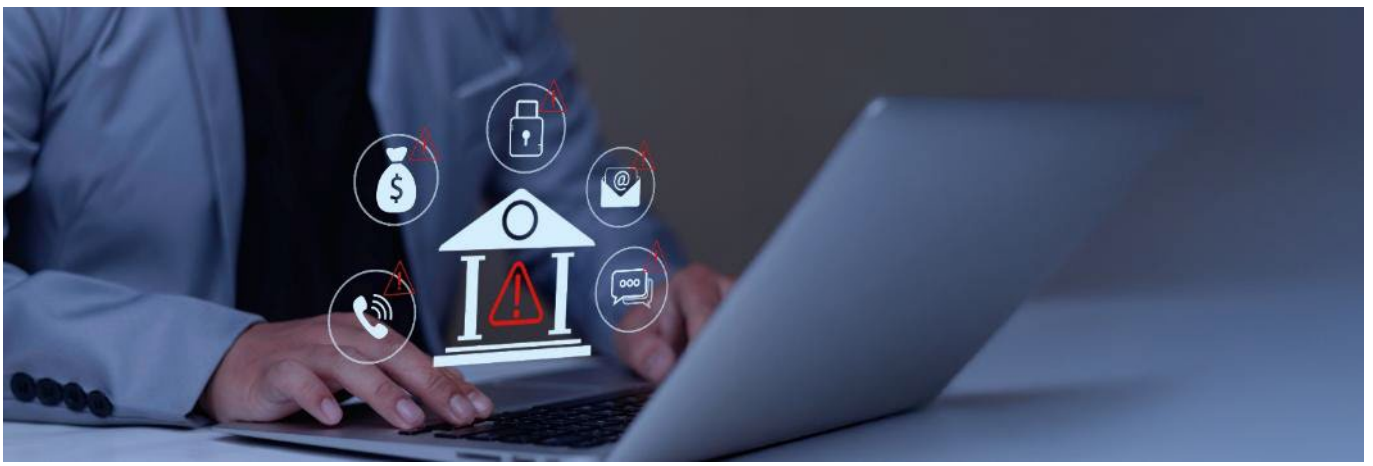
5.2 Following the money: Digital and Crypto trails

Banking and Wallet Ecosystems

Financial crime investigators in India operate within a transaction infrastructure that is simultaneously highly documented and highly fragmented. Every RTGS, NEFT, IMPS, and UPI transaction generates a log with timestamp, account numbers, transaction reference, and — for UPI — device binding and beneficiary identification data. The documentation exists. Getting to it quickly, across the multiple regulated entities that hold it, is the practical problem.

The I4C's Citizen Financial Cyber Fraud Reporting and Management System exemplifies India's progress in early fraud detection and coordinated response. It empowers victims to instantly report incidents and triggers rapid alerts to banks, leading to real-time intervention and fund freezes before losses escalate. By 2026, this platform has demonstrated its value by helping safeguard significant sums **(over INR8,000 crore recovered in reported frauds by end-2025)** and deepening inter-bank coordination. Meanwhile, fraudsters' ability to rapidly chain funds across multiple accounts in mere minutes highlights an opportunity for further innovation.[29]

Encouragingly, industry stakeholders and regulators are now exploring design-led enhancements – for example, a real-time, controlled transaction-chain access mechanism with clear legal authorisation and audit trails – to ensure investigators can trace and halt fraud flows as they happen. Due to evolved legal frameworks like the BNSS 2023 and DPDPA 2023, such a capability is widely viewed as feasible and compliant, representing the next step in aligning speed of response with the pace of digital transactions.



[27] Investigations Completed, Serious Fraud Investigation Office, Government of India, March 2026; Investigation under SFIO, Rajya Sabha Unstarred Question No. 174, Ministry of Corporate Affairs, February 2025.
[28] Master Directions on Fraud Risk Management in Commercial Banks (including Regional Rural Banks) and All India Financial Institutions, Reserve Bank of India, July 2024.
[29] Cybercrime Reporting and Investigation, Press Information Bureau, Ministry of Home Affairs, February 2026; Rajya Sabha Unstarred Question No. 1341, Ministry of Home Affairs, February 2026.

Blockchain Analytics

Cryptocurrency plays a role in Indian financial crime disproportionate to its retail adoption rate. Fraud proceeds in rupees are converted to cryptocurrency through peer-to-peer markets or semi-compliant exchanges, and the blockchain's pseudonymous structure creates a layer of obfuscation that standard banking trace cannot penetrate without specialist tools.

Blockchain analytics — following cryptocurrency flows across addresses and through mixers using well known investigation platforms has emerged as a specialist investigative discipline. All transactions on public blockchains are permanently recorded and visible, but the link between a blockchain address and a real-world identity must be established through other means. Analytics platforms maintain databases of labelled addresses — exchanges, mixers, known criminal wallets — that allow investigators to map the trajectory of funds even when the holder of a specific address is unknown.

The DeFi layer adds complexity that blockchain analytics is still developing tools to address. When funds move through automated market makers or cross-chain bridges, the transaction graph branches in ways that are harder to follow than simple wallet-to-wallet transfers. Many privacy coins — use cryptographic techniques that deliberately obscure the sender, recipient, and amount of each transaction. These represent the current frontier of crypto-based money laundering evasion, and the investigative answer requires a combination of blockchain analytics, exchange cooperation in jurisdictions where the coins are ultimately liquidated, and — in some cases — operational intelligence about the physical infrastructure supporting the fraud.

Cross-Border Financial Intelligence

Most large-scale financial frauds targeting India have an international dimension at the layering or integration stage. Criminal proceeds exit India through peer-to-peer crypto transfers, hawala channels, or trade-based mechanisms and enter the international financial system in jurisdictions with weaker AML frameworks.

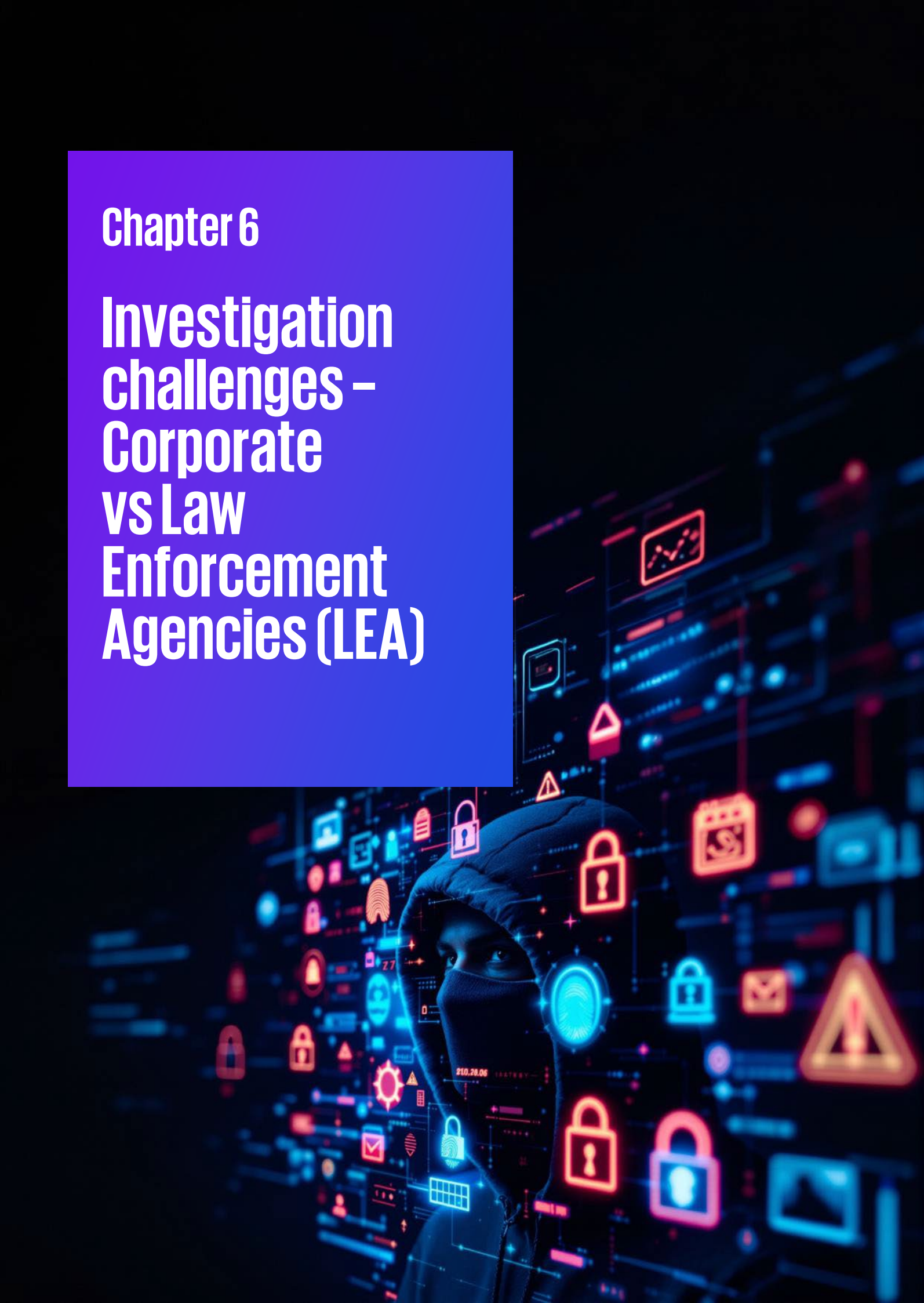
FIU-IND's membership in the Egmont Group provides access to financial intelligence sharing with over 170 member FIUs, enabling exchange of suspicious transaction data across borders without the delay of formal MLAT processes. In practice, the quality of Egmont exchanges varies by jurisdiction: mature FIUs in EU, Singapore and the UAE member states respond rapidly and substantively. Responses from less-resourced jurisdictions can take months.[30]

The structural mismatch remains: money moves in minutes; legal cooperation moves in months. Closing this gap requires pre-established bilateral agreements with key jurisdictions that include provisional freeze provisions — allowing a targeted asset freeze while formal MLAT proceedings catch up. India has such provisions with some jurisdictions under existing bilateral mutual legal assistance treaties. Extending this to prominent jurisdictions most operationally relevant to current fraud typologies — should be a near-term foreign policy and law enforcement priority.

[30] FIU-IND press release on admission to the Egmont Group, Financial Intelligence Unit–India, Ministry of Finance, Government of India; Home, Egmont Group of Financial Intelligence Units, accessed 31 May 2026; Egmont Standards and Practices for Defenses Against Money Laundering and for Countering the Financing of Terrorism, International Monetary Fund, 2005.

Chapter 6

Investigation challenges – Corporate vs Law Enforcement Agencies (LEA)



6.1 Challenges for Corporate Investigators

Data access limitations

A corporate investigator pursuing an internal fraud inquiry operates within clearly defined data-access boundaries. They can quickly scrutinise systems and records under the organisation's direct control, collaborate with willing employees, and review provided documents. Beyond this scope, reaching into personal devices or external accounts requires either the individual's consent or formal legal recourse — a built-in safeguard that upholds privacy and due process. As a result, corporate teams plan investigations carefully, often partnering with law enforcement when evidence lies outside the company's immediate reach, particularly in cases involving potential internal misconduct.

This fundamental design is evolving under India's Digital Personal Data Protection Act, 2023 (DPDPA), which reinforces transparency and purpose-specific data use. The Act encourages organisations to align their investigative processes with privacy commitments while still addressing wrongdoing effectively. With the Data Protection Board (DPB) now operational and more guidance emerging, companies are crafting even more disciplined, rights-aware investigation protocols. The trajectory is constructive: corporate investigation teams are finding ways to achieve robust fraud detection within lawful boundaries, demonstrating that internal accountability and data protection can advance hand in hand.

Legal Constraints

Corporate investigations can reveal many wrongdoings, but transforming internal findings into formal criminal cases is a complex, multi-step process that requires handing evidence to law enforcement and regulators. A company may submit a complaint to the authorities if it uncovers potential criminal conduct, but only law enforcement can decide whether to open an official investigation and pursue prosecution. As such, an internal inquiry complements but cannot replace statutory processes; indeed, in regulated industries, supervisory agencies often conduct their own parallel reviews, and a company's findings – however thorough – may be viewed as only one input rather than conclusive proof.

Legal privilege adds another dimension: if an internal investigation is led by legal counsel, some communications and reports may be protected as confidential legal advice, potentially insulating them from disclosure in private litigation. However, regulatory and enforcement bodies are empowered to demand access to internal investigative materials, and companies must carefully balance cooperation with their right to privilege. In practice, navigating these constraints is an operational reality for corporate investigators.

Internal Resistance and Governance Gaps

Fraud investigations within organisations routinely encounter resistance that is not simple obstruction but a product of institutional dynamics. A fraud involving senior management creates structural dilemmas for the investigation sponsor — typically the audit committee — because findings may expose failures of governance for which the board itself carries responsibility.

In India's corporate context, promoter-led and family-owned businesses present a specific challenge: the fraud and the company's governance may be so intertwined that a clean analytical separation is difficult. Findings that implicate promoters trigger stock exchange disclosure obligations, creditor rights, and regulatory reporting duties that create institutional pressure to limit the scope of conclusions.

6.2 Challenges for Law Enforcement Agencies (LEA)

Jurisdiction and Cross-Border Issues

Indian law enforcement agencies operate within jurisdictional boundaries that cybercrime routinely ignores. A fraud call centre operating from a country in Southeast Asia that targets Indian victims commits an offence under Indian law — but State Police have no operational reach into that country and must rely on Interpol notices, Letter of requests via MLAT, and informal diplomatic channels, all of which operate at timescales incompatible with financial crime investigation.

Within India, jurisdiction is itself contested. The most common pattern — say a frivolous call centre in Jharkhand targeting a victim in Maharashtra, with funds moving through mule accounts in Gujarat and converted via an exchange in Karnataka — requires coordination across at least four state police forces. In practice, the first investigating officer registers the case locally and investigates with limited resources, while the broader network goes largely unaddressed. I4C's coordination role addresses some of this fragmentation, but operational investigation authority remains with state police.

Lack of Skilled Manpower

Developing a top-tier digital fraud investigation team requires rare, interdisciplinary talent – blending legal insight, financial forensic, and technical prowess – a challenge faced globally. India's approach is pragmatic: specialised units at the national-level lead with deep expertise on critical cases, while an expansive effort is underway to upskill state and district cyber cells which handle the lion's share of incidents. Through targeted training programmes, knowledge-sharing networks, and modern tools that amplify available skills, capacity is steadily being built across all levels.

Innovative models are emerging, including centres of excellence for digital Forensic, shared resource hubs, public-private training partnerships, and use of automation to ease manual workloads. Recognising that experts are in demand everywhere, stakeholders are also exploring creative retention strategies – from clear career paths to collaborative industry secondments – ensuring that India's talent pipeline strengthens continuously, matching growing demand with a resilient, well-supported investigative workforce.

Technology Gaps

The tools required for modern digital financial crime investigation — mobile forensic extraction platforms, blockchain analytics suites, data engineering pipelines, cloud forensic capabilities, and AI-assisted data analysis — carry significant licensing costs and require continuous maintenance. Several state forensic science laboratories lack current licences for laptop and mobile forensic tools, which limits their ability to extract data from devices operating on newer mobile and desktop operating systems.

Blockchain analytics tools are not uniformly available outside central agency level. Any investigation touching cryptocurrency requires specialist tooling to trace fund flows across wallet chains and through mixing services. A national equipment and licensing procurement programme — analogous to the model used for DNA infrastructure and ballistic laboratories — would distribute capability more equitably and enable interoperability between state and central investigations in complex multi-jurisdictional cases.

6.3 Collaboration Gaps Across the Ecosystem

Public-Private Coordination

The data needed to investigate cyber-financial crime sits almost entirely in private sector systems — bank transaction logs, payment platform records, TSP metadata, cloud infrastructure logs. The legal authority to compel disclosure exists under BNSS 2023, but exercising it one entity at a time, through individually served notices, creates a pace of data access that is fundamentally mismatched with the pace at which fraud proceeds move.

India's fraud-fighting ecosystem is well-positioned to advance toward real-time intelligence sharing. The I4C's Citizen Financial Cyber Fraud Reporting System (CFCFRS) lays a solid foundation, rapidly connecting victims and banks to stop fraud post-incident. Building on this success, stakeholders are now exploring the next step: a coordinated, near real-time fraud intelligence network that proactively links banks, telecoms, payment operators, and cloud platforms. Designed with clear legal backing and privacy-by-design, such a framework would enable trusted, pre-authorised data exchange on emerging threats, much like proven international models. The opportunity ahead is to transform today's reactive alerts into a predictive, collective defense system, reflecting India's commitment to innovation in secure digital finance.

The fraud intelligence that flows through private sector systems is also the raw material for improving detection models across the industry. Banks, payment networks, and telecom operators accumulate data on fraud typologies, attack vectors, and mule account networks that, if shared in anonymised form through a sanctioned mechanism, would improve detection for every participant. The FIU-IND framework provides a legal basis for this exchange under PMLA. The operational design — the technical standards, governance model, and liability framework — is the missing piece.

Cross-Border Dependencies

The international dimension of Indian cyber-financial crime creates coordination dependencies that domestic mechanisms alone cannot resolve. I4C data indicates that a significant share of high-value fraud originates from organised groups operating from Eastern Europe, Southeast Asia, and West Africa.[31] Investigating these networks requires cooperation from foreign law enforcement agencies, foreign financial intelligence units, and foreign platform operators — each governed by different legal frameworks and operating under different institutional incentives.

[31] Billion-dollar cyberfraud industry expands in Southeast Asia as criminals adopt new technologies, United Nations Office on Drugs and Crime, October 2024; Move over Jamtara & Mewat, 46% of cyber fraud here stems from Southeast Asia, The Times of India, May 2024; Global Financial Fraud Threat Assessment, INTERPOL, March 2026.

The Egmont Group provides a channel for financial intelligence exchange that bypasses the formal MLAT process, but its effectiveness is uneven: mature FIUs respond quickly; less-resourced ones do not. Interpol's I-24/7 network facilitates law enforcement-to-law enforcement communication, but operational coordination — joint operations, simultaneous takedowns, asset freezes — requires bilateral agreements that India does not have with all relevant jurisdictions.

Telecom coordination is a specific gap. SIM swap fraud, digital arrest scams, and many other typologies depend on telecom infrastructure in both the perpetrator's and victim's jurisdiction. Coordinating a near-real-time response — flagging a fraudulent SIM, blocking an outbound scam call, or tracing a device identifier across borders — is not currently possible without a bilateral law enforcement-to-telecom coordination mechanism. This is an area where India's Telecom Regulatory Authority and the Ministry of Home Affairs could pursue targeted bilateral agreements with jurisdictions identified as high-risk source countries, independently of the broader MLAT process.

Chapter 7

Way forward

7.1 Building inclusive investigation capability

Skilling and Certification Ecosystem

The capability gap in cyber-financial crime investigation is fundamentally a human capital challenge. Tools can be bought, but developing investigators who both grasp legal processes and can wield technical tools effectively under courtroom scrutiny takes years. India needs a structured, stackable certification pathway for cyber-financial crime investigators that is accessible to both public and private sector practitioners. This can build on existing credentials by adding India-specific modules on the BSA 2023 evidence rules, UPI forensic, PMLA procedures, and CERT-In compliance. I4C's CyTrain platform (a MOOC-based cybercrime training, with 1,19,000+ certificates issued to police/judicial officers to date) and DSCI's training materials, as well as the COE facility of Maharashtra Cyber Security project for hands-on practice, are assets to build on. The key is a federated model where training or certification in one context (say, police) is recognised in another (private sector), encouraging mobility and knowledge sharing.[32]

Federated training recognition between police and private sector.

Shared Forensic Infrastructure

The capital cost of fully functional digital forensic labs is a barrier for many state police forces. A regional shared-service lab model could alleviate this, providing fast-turnaround digital evidence facilities serving multiple nearby states, with standard evidence submission and reporting protocols. The CFSL system already offers a template: regional CFSLs serve multiple states and accept submissions. Extending this specifically for digital forensic – with dedicated evidence intake, secure cloud analysis environments, and on-call expert support for urgent cases – is feasible within existing frameworks. The crucial requirement is earmarking dedicated resources for digital forensic within these institutions (rather than expecting existing labs to absorb the workload).

Public-Private Partnerships

The private sector holds most of the forensic data that law enforcement needs. The legal framework for compelling disclosure exists. The practical friction of issuing and serving notices across multiple regulated entities under different regulatory umbrellas remains a material investigative bottleneck.

Establishing a pre-agreed fraud data-sharing protocol among key stakeholders – I4C, NPCI, RBI-regulated banks, major telecom operators, wallet players, e-KYC service providers, and large cloud infrastructure owners – is widely seen as the next leap in India's collective fraud defence. Such a framework, which would standardise how evidence preservation requests are formatted, set clear response time targets, and authenticate each request, promises to significantly reduce current frictions. It would mirror successful international models like the Australia's Fintel Alliance, UK's Joint Fraud Taskforce, and the US FinCEN Section 314(b) programme, but tailored to India's context. The country already has the trust and institutional ties necessary to build this system; the final step is aligning stakeholders under a cross-agency mandate to formalise and operate it, a goal that is both feasible and within reach.

Regulatory compliance cannot be isolated from forensic readiness

[32] National Cybercrime Training Centre (CyTrain), National Crime Records Bureau/Indian Cyber Crime Coordination Centre, accessed 31 May 2026.

7.2 Strengthening Ecosystem Coordination (Domestic and Global)

Body/Organisation	Purpose
CERT-In	Incident response, cyber event reporting, technical controls, detection + reporting
IRDAI	Insurance fraud risk management, cyber resilience in insurers
RBI	Financial system protection, banking fraud prevention, payment security, cyber risk governance
FATF 2023	Aligns cyber fraud with AML/CFT obligations, strengthening financial traceability
INTERPOL	Enables cross-border law enforcement coordination against cybercrime networks
UNODC	Supports global capacity building and legal harmonisation for cybercrime prosecution
EU AI Act	Introduces accountability for AI-driven fraud detection and algorithmic risk management

Domestic Regulatory Drivers (CERT-In, RBI, IRDAI)

India's regulatory framework for cybersecurity and fraud risk is spread across sectors and evolving rapidly. CERT-In's April 2022 Directions impose certain incident reporting and log retention duties on a broad class of organisations (from banks to data centers to cloud providers). RBI's 2024 Master Directions on Fraud Risk Management require bank boards to strengthen fraud governance, set up early warning systems, and follow consistent fraud classification procedures. IRDAI's 2025 Insurance Fraud Monitoring Framework extends similar requirements to insurers.

While these sector-specific rules signal policy emphasis on fraud prevention and evidence readiness, they also create complexity for organisations straddling multiple sectors (e.g. a fintech handling health payment must navigate CERT-In, RBI, and possibly IRDAI obligations with different timelines and scopes).
A unified cyber-financial crime reporting framework (similar to the EU's DORA) could streamline compliance and improve data quality for regulators, but until then, companies must ensure they meet all overlapping requirements.[33]

Global Trends and Benchmarks

Internationally, policy focus on fraud and digital evidence is intensifying. FATF's 2023 report on cyber-enabled fraud emphasises that fraud proceeds cross borders swiftly and calls for stronger domestic coordination, multilateral cooperation, and improved detection controls. INTERPOL's 2026 fraud assessment highlights the rise of AI-enabled scams, global money-laundering networks, and proliferating scam call centers. UNODC's 2025 Southeast Asia brief shows how criminal syndicates exploit weak governance and uneven international readiness. While these are not laws, they shape expectations: governments, regulators, and industry are increasingly expected to coordinate and use intelligence-driven approaches against fraud.[34]

EU AI Act: Conceptual Mapping for India

The EU AI Act, which entered into force in August 2024, establishes a risk-based framework that classifies AI applications by potential harm and imposes transparency, testing, and governance requirements accordingly. AI systems used in credit scoring, fraud detection, and law enforcement biometric identification fall into its higher-risk tiers, requiring explainability, human oversight, and bias testing before deployment. The Act does not prohibit these applications; it conditions them on governance standards.

[33] Directions under Section 70B(6) 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, April 2022.
[34] Illicit Financial Flows from Cyber-enabled Fraud, Financial Action Task Force, November 2023.

India's AI governance landscape is evolving through a calibrated, sector-led approach. While a comprehensive cross-sector AI law is under development, regulatory intent is evident—particularly through SEBI's June 2025 consultation paper, which outlines principles on governance, transparency, investor protection, and human oversight for AI/ML systems in financial markets[16]. In parallel, MeitY's work under the proposed Digital India legislative framework signals a broader shift towards principle-based, risk-aware regulation that balances innovation with user safeguards.[35]

For financial crime and fraud detection, this translates into an outcome-centric regulatory approach: where AI-driven decisions result in consequential actions (e.g., account restrictions or service denial), there is increasing alignment with global best practices requiring explainability, traceability, and accessible review mechanisms.

Cross-Border Cooperation

The mechanisms for cross-border investigative cooperation in cyber-financial crime are structurally mismatched with the velocity of the crime. MLAT processes take days ; funds move in minutes. Improving this requires progress on multiple tracks simultaneously: bilateral agreements with key jurisdictions — Singapore, UAE, UK, and the US — that include provisional freeze provisions; Egmont Group exchanges for financial intelligence that bypass the MLAT process for intelligence-only purposes; and direct law enforcement-to-law enforcement protocols through Interpol and bilateral cooperation agreements.

India's engagement with FATF — in the context of its mutual evaluation — creates both an obligation and an opportunity. Meeting FATF's effectiveness criteria requires demonstrating not just that the legal framework exists but that it produces results: asset recoveries, prosecutions, and financial intelligence that leads to actionable enforcement outcomes. The mutual evaluation process provides external accountability that domestic political processes have difficulty replicating.

Implications for Corporate Leadership

Regulatory compliance can no longer be isolated from fraud investigative capabilities. Controls that improve authentication, metadata granularity, transaction verification, logging, customer communication, or third-party oversight also improve the ability to investigate incidents. Conversely, poor forensic readiness can become a regulatory liability – it may impair breach assessments, delay customer redress, hamper suspicious activity reporting, or lead to compliance violations. A forward-looking approach means treating policy requirements as inputs into capability design (not just post-facto checklists). The organisations best prepared for future scrutiny will be those that integrate fraud risk strategy with corporate governance, privacy management, data governance, and strong evidence practices.

[35] Consultation Paper on guidelines for responsible usage of AI/ML in Indian Securities Markets, Securities and Exchange Board of India, June 2025.

7.3 Strategic roadmap and initiatives

For **corporates and financial institutions**, the immediate priority is to conduct a thorough Digital Forensic Readiness Assessment (DFRA) and implement strong volatile evidence preservation procedures – clearly documented, rehearsed, and tested at least annually. These cost relatively little but have an outsized impact when an incident strikes. Recent May 2026 Supreme Court judgment also implies third-party forensic experts can more readily validate electronic evidence (like emails, logs, chat records) for legal proceedings, and well-prepared companies – with access to certified digital forensic experts – can handle evidence preservation and certification in-house or via trusted partners instead of waiting for overburdened government labs.

For **BFSI entities**, invest in India-specific fraud analytics tuned to current threats: e.g. patterns in UPI usage, multilingual social engineering cues, known mule network behaviours – rather than relying purely on generic global models that might miss local fraud signatures. Additionally, sharing anonymised fraud intelligence across the industry (via FIU-IND or sectoral forums, as permitted by PMLA provisions) can improve collective detection capabilities.

At the **board and C-suite level**, institute a formal fraud risk oversight function. This means clear escalation thresholds for major incidents, explicit engagement in significant fraud cases, and direct accountability for the adequacy of fraud controls. Fraud risk should be treated not as a mere compliance item but as a governed risk domain with named ownership. Some of these activities are required to be performed under Companies Act 2013 requirements and need focus to make fraud oversight function a competitive advantage for the organisations.

For **regulators and public agencies**, one of the most impactful steps in the near term is establishing a real-time data-sharing infrastructure for fraud evidence. This doesn't necessarily need new laws – BNSS 2023 Section 94 and RBI's oversight of payment participants provide legal basis – but it does need operational design and commitment from RBI, TRAI, MEITY (for telecom, internet, and tech platforms) to mandate participation.

Courts would benefit from **clear, authoritative guidance on digital evidence standards**. Certain questions remain open like handling cloud evidence chain-of-custody, standards for hash verification of AI-derived evidence, weight of blockchain analytics as evidence, etc. A practice direction or guidelines could help lower courts apply consistent standards on these technical points, reducing uncertainty that currently can be exploited by defendants to challenge evidence.

Investments in technology and talent: Following technology investments promise high returns for investigation effectiveness:

1. A **national case management and digital evidence platform** for all state and central investigative agencies, with standardised chain-of-custody tracking and integration with court IT systems.
2. A **shared blockchain analytics capability** (centrally procured) accessible to state cyber cells on a case-by-case basis, so that every VDA/crypto-linked case can leverage best-in-class tracing tools (rather than each state negotiating separately for expensive licenses).
3. An **AI-assisted initial triage tool** customised for Indian investigative data – e.g., one that can ingest unstructured data like CDRs, IPDRs, bank statements, UPI logs, complaint data, social media accounts, and produce a structured summary of a case for investigators under tight timeframes.
4. Setting up an **accreditation framework** or professional body to vet and credential private forensic practitioners and labs will standardise forensic certification process.

On the human capital side, **retention** is as critical as recruitment. Consider creating specialist career tracks within the LEAs for certified cybercrime and digital forensic investigators, with incentives (competitive pay scales, promotion paths that don't force leaving the technical specialisation, recognition for court testimony and contributions to forensic methodologies). This could mitigate brain drain to private companies.

In addition, continued **public awareness** efforts yield high returns in reducing the incidence of fraud in the first place. Various initiatives by MHA and State Police about public awareness – all these reach large audiences. Institutionalising such efforts as a funded, ongoing programme (rather than reactive responses to specific scam outbreaks) can steadily shrink the pool of potential victims, diminishing fraudsters' success rates.

7.4 Building Next-Generation Forensic Readiness

Forensic readiness refers to an organisation's ability to preserve, access, analyse, and use relevant evidence quickly and reliably when fraud occurs. In many institutions, this remains underdeveloped. Assets may be hidden, patches may be outdated, logging may be inconsistent, retention periods too short, escalation triggers unclear, forensic support is missing, retainers are non-existent, access rights fragmented, responsibilities overlap and decision dilemmas exists, and investigative playbooks either outdated or absent. Yet the current digital and threat environment leaves little room for such weaknesses.

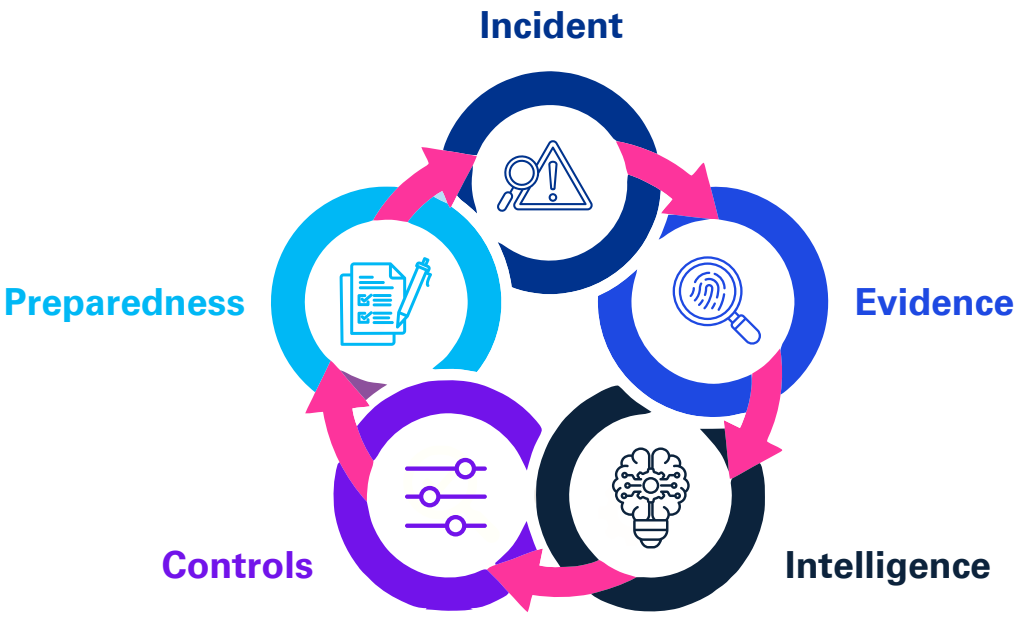
> **Forensic readiness must be a core operational requirement...**

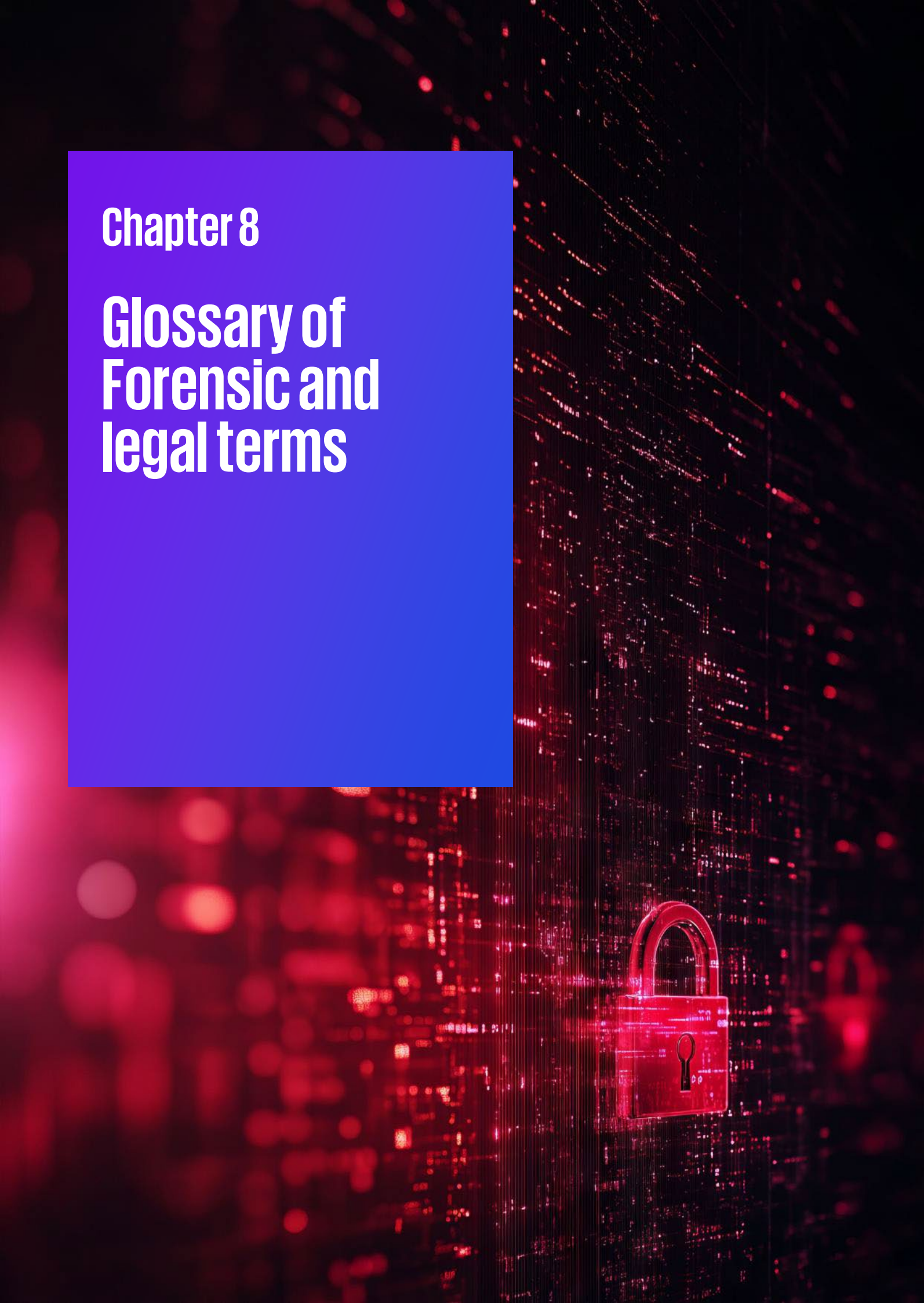
Modern digital fraud demands that organisations embed forensic readiness as a core operational requirement, not merely a reactive afterthought. This means elevating investigative ability into a strategic resilience pillar, championed at the Board and CXO level. Cross-functional alignment across fraud risk, cyber security, legal, and compliance is essential: teams must share clear escalation protocols and evidence standards to ensure swift, coordinated responses when incidents occur.

Organisations should embrace a staged roadmap for capability enhancement. First, baseline assessments can pinpoint gaps—critical evidence sources, log retention, incident-to-investigation handoffs, and third-party dependencies. Next, targeted control improvements in areas such as identity assurance, payment integrity, cloud visibility, and third-party risk management strengthen both prevention and investigative clarity. These measures help shift the focus from isolated fixes to an integrated framework that supports repeatable, auditable investigations and robust fraud containment.

At the ecosystem level, collaboration and continuous learning are pivotal. By building common reporting frameworks, sharing typologies, and enabling faster public–private coordination, industry and regulators can stay ahead of interconnected threats. The goal is to shorten response times across borders and between institutions, reflecting the reality that no single entity can counter pervasive cyber-enabled fraud alone.

Ultimately, the most resilient organisations will be those that build strong 'institutional memory.' They systematically preserve useful evidence, use it to learn and improve, then feed those insights back into better controls and training. By developing this kind of closed-loop system linking detection, investigation, governance, and trust, organisations strengthen both their business resilience and regulatory credibility over the long term. This next-generation approach transforms fraud investigation from an emergency response into a continuous cycle of defence and improvement — that capability will become increasingly central to business resilience, regulatory confidence, and public trust.





Chapter 8

Glossary of Forensic and legal terms

1. **Account Takeover (ATO):** Unauthorised access to and control of a financial or payment account by a third party, typically following credential compromise.
2. **Anti-Forensic:** Techniques used by a perpetrator to destroy, conceal, or alter digital evidence before or after collection by investigators.
3. **Call Detail Record (CDR):** A telecom operator's log of telephone calls made and received, including originating and terminating numbers, call duration, timestamps, and cell tower identifiers.
4. **Chain-of-Custody:** A documented record of the collection, transfer, analysis, and disposition of evidence, designed to ensure integrity and admissibility.
5. **DeFi (Decentralised Finance):** A category of financial services built on public blockchain networks using smart contracts, operating without central administrators or intermediaries. The absence of a central operator means there is no entity to compel compliance with legal or regulatory demands.
6. **Deepfake:** Synthetic audio or video media in which a person's likeness or voice has been replaced or manipulated using deep learning models, typically without their consent.
7. **Digital Arrest Fraud:** A social engineering fraud typology in which a perpetrator impersonates a law enforcement officer and convinces a victim to remain in continuous video contact while transferring funds under threat of fabricated criminal charges.
8. **Fileless Malware:** Malicious code that executes entirely in a computer's volatile memory (RAM) without writing files to disk, making detection and post-incident forensic recovery significantly more difficult.
9. **Forensic Image:** A bit-for-bit copy of a storage device's entire contents, including deleted files and unallocated space, verified by a cryptographic hash value. The industry standard formats are E01 and AFF4.
10. **MLAT (Mutual Legal Assistance Treaty):** A bilateral agreement between states that establishes a formal mechanism for obtaining evidence, locating fugitives, and executing judicial requests across national borders.
11. **Money Mule:** An individual who, wittingly or unwittingly, receives and transfers criminally derived funds, typically retaining a small percentage as compensation. Constitutes an offence under the Prevention of Money Laundering Act 2002.
12. **NFT (Non-Fungible Token):** A unique digital asset recorded on a blockchain. In financial crime contexts, NFTs are used for wash trading (artificially inflating price history) and as a money laundering mechanism through transactions between criminal-linked wallets.
13. **Section 63 Certificate (BSA 2023):** A certificate required under Section 63 of the Bharatiya Sakshya Adhiniyam 2023 (formerly Section 65B of the Indian Evidence Act) for the admissibility of electronic records in court.
14. **SIM Swap:** A fraud in which a perpetrator convinces or bribes a telecom provider to transfer a victim's phone number to a SIM card under the fraudster's control, enabling interception of OTP-based authentication messages.
15. **Timestomping:** An anti-forensic technique that modifies the metadata timestamps (creation, modification, access) of files to disguise the true timeline of computer activity.
16. **Trade-Based Money Laundering (TBML):** The use of international trade transactions — through invoice manipulation, misrepresentation of goods, or falsified shipping documents — to move, conceal, and integrate criminal proceeds across jurisdictions.
17. **Volatile Evidence:** Digital evidence that exists only in active system memory or depends on an active network connection and is irrecoverably lost if the system is powered off or the connection terminated.

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialization, and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

About KPMG in India

KPMG entities in India, are professional services firm(s). These Indian member firms are affiliated with KPMG International Limited. KPMG was established in India in August 1993. Our professionals leverage the global network of firms, and are conversant with local laws, regulations, markets and competition. KPMG has offices across India in Ahmedabad, Bengaluru, Chandigarh, Chennai, Gurugram, Hyderabad, Jaipur, Kochi, Kolkata, Mumbai, Noida, Pune, Vadodara, and Vijayawada.

KPMG entities in India offer services to national and international clients in India across sectors. We strive to provide rapid, performance-based, industry-focused and technology-enabled services, which reflect a shared knowledge of global and local industries and our experience of the Indian business environment.

KPMG in India contacts:

Akhilesh Tuteja
Global Head – Cyber Security
E: atuteja@kpmg.com

Mohit Bahl
Partner and Head
Risk and Integrity Advisory
E: mbahl@kpmg.com

Suveer Khanna
Partner and Head
Forensic Services
E: skhanna@kpmg.com

Mustafa Surka
Partner
Forensic Services
E: mustafasurka@kpmg.com

Gagan Budhiraja
Partner
Forensic Services
E: gaganbudhiraja@kpmg.com

FICCI contacts:

Mr. Sumeet Gupta
Deputy Secretary General, FICCI

Mr. Akhil Gupta
Director, FICCI
E: akhil.gupta@ficci.com

Ms. Aastha Gupta
Senior Assistant Director, FICCI
E: aastha.gupta@ficci.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia