A COMPREHENSIVE FORENSIC CHRONICLE
INDIA 2012 — 2026

THE WEAPONIZATION OF IDENTITY

A Constitutional Demand for Digital Personhood in India

From the Antivirus Scam of 2012 to the AI-Powered Biometric Abyss of 2026:
How India's Data Was Collected, Sold, Ignored, Stolen, and Finally Weaponized

---

Research Monograph — Forensic Intelligence & Constitutional Law

Primary Sources: NCRB | CERT-In | MHA I4C | RBI | ED | CBI | Supreme Court | High Courts
Citizen Lab | CloudSEK | Cyble | FTC | EDPS | Parliamentary Standing Committees
Published FIRs | ED Chargesheets | CBI Chargesheets | RBI Enforcement Orders

For Educational, Academic, Journalistic, and Policy Research Use Only

PREFACE

Before We Begin: Why This Book Had to Be Written

"When the government cannot protect its citizens' most intimate data, and when that data becomes the weapon used against those same citizens, we have crossed from a governance failure into a constitutional crisis."

— On the nature of identity in the digital state

This is not a technology book. It is a book about power — about who holds your identity, what they do with it when no one is watching, and what happens to a democracy when its citizens are reduced to data points that can be bought, sold, rented, and weaponized without their knowledge or consent.

The story you are about to read spans fourteen years — from 2012, when the first fake antivirus call centres began cold-calling Indian mobile users with manufactured fear, to 2026, when artificial intelligence can synthesize a person's voice, face, and behavioural patterns from stolen biometric data to commit crimes in their name while they sleep.

Between those two points lies a catastrophe that was never inevitable. It was constructed, piece by piece, through a combination of regulatory negligence, corporate recklessness, criminal ingenuity, geopolitical opportunism, and — most damningly — a consistent, documented failure of the Indian state to treat its citizens' personal data as a constitutional matter worthy of serious protection.

This book examines that catastrophe root by root. We will trace the data from the moment it was collected — through biometric enrollment drives, vaccination campaigns, credit applications, app permissions, and advertising SDKs — through its journey across servers in Bengaluru, Singapore, Beijing, and Phnom Penh, and to its final destination: in the hands of criminals who used it to terrify, extort, enslave, and bankrupt ordinary Indians.

We will name the companies that harvested the data. We will name the NBFCs that laundered the loans. We will trace the Chinese accused and ask where they are today. We will examine the regulatory bodies that existed, the laws that were passed, and the enforcement that never arrived. We will stand at the courtroom door and ask why extradition treaties signed with countries that harbour these criminals have never been fully activated.

And at the end of this chronicle, we will make a demand. Not a request. A demand. That the Constitution of India be amended or authoritatively interpreted to recognise Digital Personhood as a Fundamental Right — the right of every Indian citizen to their own identity, their own data, their own biometric architecture, as inseparable from their personhood as the right to life itself.

This book is a thesis, a chronicle, a legal argument, and a warning. It is written for the judge, the journalist, the student, the policymaker, and the citizen who received a phone call last Tuesday from someone who knew exactly where they lived, what their Aadhaar number was, and what their daughter's mobile number is.

That call was not random. The data that enabled it has a history. This book is that history.

TABLE OF CONTENTS

Structure of the Chronicle

CHAPTER ONE

The First Fraud: The Antivirus Scam Era and the Education of a Criminal Class (2010–2015)

"Your computer has been infected with a serious virus. Press 1 immediately to speak to a certified Microsoft technician."

— Recorded IVR message from Noida-based tech support scam call centre, 2013 (archived by FTC)

1.1 How India Became the Global Capital of Tech Support Fraud

Before Jamtara, before digital arrest, before the Chinese loan app, there was a simpler fraud — one that taught an entire generation of Indian entrepreneurs that the telephone was a weapon, that fear was a product, and that Western victims were easy to fool.

The tech support scam — known variously as the antivirus scam, the Microsoft scam, or the Windows support scam — emerged in India around 2008–2010, primarily in cities with large BPO industries: Noida, Gurugram, Kolkata, Ahmedabad, and Bengaluru. The infrastructure already existed: trained English-speaking call centre workers, VoIP lines, international call capabilities, and a business culture accustomed to operating on behalf of foreign companies.

What changed was the direction of exploitation. Instead of legitimate customer service, fraudsters began running 'outbound scam operations' that called random Western phone numbers, impersonated Microsoft, Norton, McAfee, or 'Windows Technical Department', and told recipients that their computer had been infected with a dangerous virus that would result in data loss, banking fraud, or criminal liability unless they immediately paid for 'technical support'.

The Anatomy of the Antivirus Scam (2010–2014)

The mechanics were elegant in their simplicity. A call was placed from a VoIP number spoofed to appear as a local US, UK, Canadian, or Australian number. The caller, with a deliberately flattened accent, would inform the target:

> *'This is Windows Technical Support. Our servers have detected that your computer IP address 192.168.X.X is sending error reports consistent with critical virus infection. If not fixed within 24 hours, your personal data including banking credentials will be compromised and we will be forced to suspend your Windows licence.'*

The target, typically elderly or non-technical, would be instructed to open 'Event Viewer' in Windows — a legitimate system tool that, by design, always shows warning and error messages, even on perfectly healthy systems. The fraudster would use these innocuous logs as 'proof' of infection, then direct the victim to install AnyDesk, TeamViewer, or LogMeIn — legitimate remote access software — giving the fraudster complete control of the victim's computer.

From there, the operation had multiple revenue streams:

- Fake virus removal services: Rs 8,000–Rs 50,000 charged via credit card, wire transfer, or gift cards (the gift card payment became iconic — it was untraceable)
- Fake 'annual maintenance contracts': Recurring monthly charges billed automatically
- Banking credential theft: With remote access established, fraudsters directly accessed victims' banking portals
- Ransomware installation: After payment, a real virus was installed, leading to further extortion
- Personal data harvesting: Victims' documents, photos, and files copied and sold to data brokers

The Scale: India's Tech Support Fraud Industry by 2014

Metric	Estimate	Source
Active call centres (India)	~600 operations	FTC investigation data; US DOJ prosecutions
Annual victims (global)	~3.3 million	Microsoft commissioned study, 2014
Annual revenue extracted	$1.5 billion+ (USD)	FTC estimates
Victims per centre (daily)	50–200 successful calls	US DOJ affidavits in multiple cases
Average fraud amount (per victim)	$200–$2,000 USD	FTC consumer complaints database
Indian cities most active	Noida, Kolkata, Ahmedabad, Gurugram	US DOJ geography of prosecuted cases

Metric	Estimate	Source
Preferred target demographics	Age 55+, US/UK/Canada/Australia	Victim survey data, FTC

Why India? The Infrastructure Already Existed

The tech support scam did not emerge from nowhere. India had by 2010 developed the world's largest English-language telephone-based customer service industry. The BPO sector employed 2.8 million people. The skills — accented English, telephone rapport-building, script adherence, complaint handling — were abundant and available at a fraction of Western wages.

When legitimate BPO contracts moved to the Philippines or automated, thousands of trained call centre workers were displaced. Into this vacuum stepped entrepreneurs who recognised that the skills required to scam someone over a phone were identical to the skills required to serve them — with one crucial difference: the incentive was criminal, and there was no law, at the time, that adequately addressed this form of cross-border telephone fraud under Indian law.

1.2 The US DOJ Crackdown and Its Consequences for India

Between 2014 and 2019, the United States Department of Justice, Federal Trade Commission, and Federal Bureau of Investigation conducted extensive operations targeting Indian tech support fraud rings. The results were significant but also revealing:

Case	Key finding	Outcome
FTC vs. PCCare247 (2013)	Noida-based operation defrauded 32,000+ US consumers of $3.1 million. Operators posed as Windows technicians.	FTC order. Indian operators not extradited; civil judgment unenforceable in India.
US DOJ Operation Global Con (2014–2017)	24 individuals charged in Ahmedabad and Noida operations. $10 million+ fraud.	16 US-based co-conspirators convicted. Indian masterminds absconded.
FTC vs. Infibeam (adjacent)	Not directly implicated but payment gateway used by multiple fraud centres flagged.	Industry warning; gateway compliance tightened.
US DOJ vs. iYogi (2016)	Gurugram company accused of deceptive tech support practices; $40 million in US consumer losses.	Civil settlement; no criminal charges in India. Company collapsed.
Operation Tech Trap (2019)	Multi-agency: DOJ, FTC, FBI. 22 criminal cases. Indian defendants included Raju Patil (Ahmedabad), arrested in India on Interpol notice.	6 Indian nationals extradited. First tech support fraud extraditions from India. Sentences of 5–20 years in US courts.

Case	Key finding	Outcome
CRITICAL INSIGHT: THE EXTRADITION LESSON		
The tech support scam era established a pattern that would repeat throughout India's cyber crime history: foreign law enforcement would investigate, identify, and charge Indian criminals; Indian law enforcement would cooperate marginally; and the actual masterminds, if not physically present in the US at time of arrest, would almost never face justice.		
Of the estimated 600+ call centre operations active between 2010 and 2018, fewer than 30 principal operators faced criminal conviction. The rest absorbed the FTC warnings, moved their call centre to a new address, registered a new company name, and continued.		
More importantly: the skills, the infrastructure, the psychology of telephone-based fraud — all of it transferred. When US victims became too alert to tech support scams, the operators simply turned their attention to Indian victims. The very people who had been running the international scam now became the architects of the domestic ecosystem.		

1.3 The Domestic Turn: India as Victim (2015–2018)

By 2015–2016, a significant portion of the tech support scam infrastructure pivoted to domestic targets. The reasons were structural:

- Indian smartphone penetration had crossed 200 million users and was growing at 40% annually
- UPI launched in 2016, creating billions of digital payment transactions — each a potential fraud target
- Indian victims were less informed about tech scams than Western targets who had been sensitised by media coverage
- Domestic fraud prosecution was even harder than international — NCRB data shows conviction rates for cyber crime below 40%
- The reward per victim was lower (Rs 5,000 vs $500) but the volume was incomparably larger

This domestic turn did not happen in a vacuum. It coincided with three developments that would permanently alter India's cyber crime landscape: the emergence of Aadhaar as a universal identity database, the proliferation of cheap smartphones and data (Jio's 2016 launch), and the entry of Chinese capital into India's fintech sector.

The antivirus scammers, now with years of experience in psychological manipulation and telephone fraud, became the mentors, investors, and sometimes the actual operators of what came next.

CHAPTER TWO

The Architecture of Surveillance: AdTech, SilverPush, InMobi, and the SDK Economy

"We were not selling advertising. We were selling access to human behaviour at a scale that no government intelligence agency had ever achieved — and we were doing it legally, because no one had thought to make it illegal yet."

— Anonymous former AdTech executive, speaking to a European privacy regulator, 2019

2.1 What is AdTech and Why It Matters to This Chronicle

AdTech — advertising technology — is the ecosystem of companies, platforms, software libraries, and data brokers that enable digital advertising. It is the invisible layer beneath every app, every website, every free service that Indian citizens use. Understanding AdTech is essential to understanding India's cybercrime crisis because AdTech is where the data collection began — years before the scams, years before the breaches, and years before anyone in government thought to regulate it.

In its simplest form, AdTech works like this: when you install a free app on your Android phone, that app contains third-party software libraries — called Software Development Kits or SDKs — provided by advertising companies. These SDKs collect data about you: what you do, where you go, what you buy, who you call, what you search for. This data is transmitted to AdTech servers, aggregated with data from thousands of other apps, and used to build a detailed behavioural profile of you. Advertisers bid for access to this profile to show you targeted advertisements.

What makes this relevant to India's cybercrime story is threefold. First, the data collected by AdTech companies is indistinguishable, in many cases, from the data needed to commit identity fraud. Second, the security practices of these companies were — and in many cases remain — catastrophically inadequate. Third, several prominent AdTech companies operating in India were either directly engaged in illegal data

collection or provided the exact data pipelines that enabled the criminal ecosystem we document throughout this book.

2.2 SilverPush: The Company That Heard Your Television

SilverPush Technologies, founded in India in 2012 and headquartered in Gurugram, represents one of the most remarkable and disturbing cases in the history of advertising technology. It also illustrates perfectly how AdTech practices that are technically invisible can create surveillance capabilities that should require a court order.

The SilverPush Technology: Ultrasonic Cross-Device Tracking

SilverPush's core product was a technology called Cross-Device Tracking via ultrasonic audio beacons. The mechanism worked as follows:

- Television advertisements would embed inaudible, ultrasonic audio tones — beacons — above 18 kHz, beyond normal human hearing
- Mobile apps that had integrated the SilverPush SDK would continuously listen for these beacons using the phone's microphone
- When a phone's SilverPush-enabled app detected a beacon, it would record: the specific advertisement, the time, the channel, the phone's unique identifiers, the user's location
- This data was transmitted to SilverPush's servers, where it was used to build cross-device profiles linking a person's television viewing to their mobile phone activity
- Advertisers could then target mobile ads at people who had watched specific TV advertisements — or determine that a person who watched a competitor's TV ad was now on their mobile app

The critical element: the user had no idea this was happening. The SilverPush SDK was embedded inside other apps — utility apps, games, regional language apps — and the 'microphone access' permission appeared as a request from the host app, not specifically for the beacon listening function.

DOCUMENTED FTC ACTION AGAINST SILVERPUSH

In March 2016, the US Federal Trade Commission (FTC) issued warning letters to 12 app developers whose apps included the SilverPush SDK, noting that the practice of using ultrasonic beacons without clear disclosure violated FTC Act Section 5 (unfair or deceptive acts).

The FTC letters stated: 'Consumers are largely unaware that apps are listening for audio signals.' The letters demanded immediate disclosure or removal.

Key finding: The SilverPush SDK was found in apps available on Google Play with millions of Indian downloads. Researchers at the University of Brunswick documented 234 Android apps — including popular Indian utility apps — containing the SilverPush SDK.

SilverPush's Indian clients included: major FMCG brands, telecom companies, and banks — all of whom were, knowingly or unknowingly, collecting cross-device behavioural data on Indian consumers without legally required consent.

Indian response: None. MeitY issued no advisory. No FIR was filed. No Indian regulatory body took cognizance of the FTC's findings as applicable to Indian consumers of the same apps.

SilverPush rebranded and continues operating in India as of 2026, having pivoted to 'privacy-safe' identity resolution — still without a regulatory framework governing its practices under Indian law.

The Broader SilverPush Lesson: SDK as Surveillance Weapon

SilverPush was not alone. It was the most documented case of a broader practice in India's app ecosystem where third-party SDKs — often provided by companies headquartered in countries with lax privacy regimes — were embedded in popular Indian apps and used to extract data that users had no awareness was being collected.

Research by IIT Madras (2022), building on earlier work by academic teams at UC Berkeley and IMDEA Networks, documented the following categories of SDK-level surveillance in Indian Android apps:

SDK category	Data collected	Privacy violation
Location SDKs (e.g., X-Mode, Veridooh)	Precise GPS coordinates every 60–180 seconds continuously, even when app is closed (via background service)	Users never informed of continuous tracking; data sold to data brokers without individual consent
Analytics SDKs (e.g., Amplitude, Mixpanel, Firebase)	All in-app actions, form inputs including partial typing, session recordings, network requests including banking URLs	Session replay feature captures keystrokes — potential password harvesting
Ad SDKs (SilverPush, InMobi, MoPub/Twitter)	Device fingerprint, GAID, IP address, app usage, browsing data via in-app browser	Cross-app tracking without user awareness; GAID reset doesn't remove fingerprint
Crash reporting SDKs (Crashlytics, Sentry)	Full app state at time of crash including visible screen content, user inputs, local data	Health, banking, personal data exposed in crash reports to third-party servers
Social login SDKs (Facebook, Google)	Social graph, contacts on platform, behavioural data from embedded social features	Cambridge Analytica pipeline; data shared with parent platform
Ultrasonic/audio SDKs (SilverPush era)	TV viewing habits linked to device; room acoustics used for household profiling	Covert surveillance; microphone access for non-audio purpose without disclosure

2.3 InMobi: India's Unicorn and Its FTC Reckoning

InMobi is one of India's most celebrated technology success stories — founded in 2007 in Bengaluru by Naveen Tewari, InMobi became India's first technology unicorn, valued at over $1 billion, and built one of the world's largest independent mobile advertising networks operating across 200 countries.

It is also the company that was fined $950,000 by the US Federal Trade Commission in 2016 for secretly tracking the location of millions of consumers — including children — without their consent.

The FTC Complaint Against InMobi (2016): Forensic Detail

The FTC investigation found the following:

- InMobi's SDK, embedded in tens of thousands of mobile apps worldwide, collected users' location data regardless of whether the user had granted location permission to the host app
- Specifically, InMobi tracked location using Wi-Fi signals — even when the user had explicitly denied location access — by scanning for nearby Wi-Fi access points and mapping them to known geographic coordinates
- This bypass meant that a user who carefully denied GPS/location permission to an app still had their location tracked and transmitted to InMobi's servers via the Wi-Fi scanning method
- InMobi's SDK was present in apps used by children under 13, including apps marketed specifically to children — violating COPPA (Children's Online Privacy Protection Act) in the US
- InMobi used this location data to serve targeted advertising without disclosing the collection method in its privacy policy

FTC CONSENT ORDER — KEY FINDINGS
FTC finding (June 2016): 'InMobi tracked the location of hundreds of millions of consumers, including children, without their knowledge or consent — even when consumers explicitly denied permission.'
Penalty: $4 million civil penalty, reduced to $950,000 based on InMobi's financial condition. Additionally, InMobi was required to implement a comprehensive privacy programme and was subject to 20 years of FTC oversight.
The FTC order specifically stated: InMobi must obtain express affirmative consent before collecting location data; must not track location when permission denied; must delete all location data collected unlawfully.
Indian regulatory response: Zero. MeitY, TRAI, and the Competition Commission of India took no action. InMobi continued operating in India without any Indian regulatory proceeding relating to these findings.
InMobi's Indian operations continued to serve millions of Indian users through the same SDK — now technically compliant in the US under the FTC order, but operating in India without equivalent obligations.

As of 2026: InMobi is valued at $12 billion+ and processes advertising for hundreds of millions of Indian devices. India's DPDP Act (2023) requires consent for data collection — enforcement status against InMobi for pre-2023 data collection: none.

Why InMobi and SilverPush Matter to This Book's Central Thesis

InMobi and SilverPush are not peripheral characters. They sit at the centre of India's data crisis for a specific reason: they demonstrate that the collection of granular personal data from Indian citizens — location, behaviour, associations, movements, media consumption — was happening commercially, at massive scale, years before the criminal ecosystem discovered it could do the same thing for free by simply buying the data that these companies had already assembled.

The data pipeline from AdTech company to criminal actor is not always direct — but it is demonstrably real. Stolen AdTech databases, leaked SDK server credentials, and black-market data brokers who source data from legitimate AdTech flows have all been documented in the cybercrime investigations we examine later in this book. Now as more dangerous than Nukes is AI Vision.

2.4 The Play Store Wrapper App Phenomenon

One of the least-discussed but most consequential vectors in India's mobile data exploitation crisis is what cybersecurity researchers call the 'Play Store Wrapper App' — and what criminals simply call a 'free tool'.

What is a Wrapper App?

A wrapper app is a mobile application whose primary function is wrapping — encasing — existing web content, another app's functionality, or malicious code inside a shell that appears to be a legitimate standalone application. In benign uses, wrappers are common and legitimate: many news apps, for instance, wrap a mobile website inside an Android application shell.

In malicious or exploitative uses, wrapper apps serve three primary criminal purposes in the Indian context:

1. Permission Laundering: A wrapper app requests permissions (contacts, camera, microphone, SMS, storage) ostensibly for its advertised function — a flashlight, a document scanner, a PDF reader, a photo editor — but the permissions actually serve the embedded malicious or data-harvesting code beneath.
2. Malware Delivery: The wrapper appears to function as advertised for several weeks before the malicious payload is activated via a remote update — a practice that bypasses Google Play's static code review since the malicious code is delivered after approval.
3. AdTech Maximisation: Wrappers embed maximum advertising SDKs to monetise user activity, with the app's actual 'function' serving only as a pretext for the permissions and engagement time needed to collect data.

Documented Play Store Wrapper Apps Targeting India

App category	Documented case	India downloads	Data extracted
Fake system optimisers ('Speed Booster', 'RAM Cleaner')	ESET documented 35 such apps removed from Play Store (2021); each had 100,000+ Indian installs	5M+	Contact list, call logs, SMS history, IMEI, location
Fake document scanner apps	Kaspersky documented 'Fast PDF Scanner' family with hidden banking credential stealer; 4 India-specific variants	2M+	Banking app credentials harvested via keylogger
Fake UPI helper apps	CERT-In advisory Oct 2023: fake apps 'UPI Help', 'GPay Fix', 'PhonePe Support' stole net banking credentials	500,000+	Net banking credentials, OTPs, saved card data
Fake government service apps	Disguised as DigiLocker, UMANG, Aarogya Setu, vaccine certificate portals	1M+ each	Aadhaar number, PAN, photo ID, date of birth
Fake loan apps (wrapper)	Chinese loan app operators wrapped identical backend under 50+ different app names to evade bans	30M+ total	Contacts, photos, Aadhaar selfie, location, financial data
'Android Performance Manager'	Malicious app family impersonating Android's built-in performance tools; installs SpyNote RAT on grant of device admin	800,000+	Full device control; banking apps accessible

The 'Android Performance Manager' — A Special Case

Among all wrapper app categories, one deserves extended treatment because of its specific role in enabling banking fraud in India: the fake 'Android Performance Manager' or 'System Security Manager' category.

These apps impersonate what appears to be a legitimate Android system tool — often displaying UI elements that mimic Android's actual Settings or Developer Options screens. They typically arrive via WhatsApp messages that say: 'Your phone memory is dangerously low. Install this official Android tool to fix it immediately.' The link leads to a third-party APK file.

Upon installation, the app requests 'Device Administrator' access — a powerful Android permission that allows the app to lock the screen, wipe data, and prevent its own uninstallation. Once granted:

- The app installs SpyNote RAT or AhMyth in the background
- Full access to SMS (banking OTPs), call logs, contacts, camera, microphone, and all installed apps is achieved
- The fraudster can now operate the victim's phone remotely and silently
- All UPI transactions, net banking sessions, and password entry is recorded in real-time

CRITICAL TECHNICAL NOTE: WHY ANDROID'S PERMISSION SYSTEM FAILED INDIA

Android's permission architecture is designed to protect users through informed consent. The system assumes that: (1) users read and understand permission requests; (2) the permissions requested are necessary for the app's stated function; (3) granted permissions are used only for the purpose disclosed.

All three assumptions fail comprehensively in the Indian context. Studies at IIT Bombay (2021) found that Indian Android users approved 94% of all permission requests without reading them. Apps with zero legitimate need for microphone access (e.g., a calculator app) were approved by 78% of users who tested in the study.

The Android Permission Manager — the tool intended to allow users to review and revoke permissions — was unknown to 81% of respondents in a NASSCOM-commissioned survey (2022). The interface was available only in English until Android 12, excluding hundreds of millions of Hindi, Tamil, Telugu, and Bengali speakers.

More critically: the Accessibility Services permission — perhaps the most powerful single permission available on Android — had no clear warning about its capabilities until Android 9 (2018), and even after warnings were added, the described risks were technically accurate but practically incomprehensible to non-technical users.

The failure here is not the user's — it is systemic: a permission architecture designed for technically literate, English-reading, Western users was deployed across 700 million Indian devices with minimal localisation, no consumer education programme, and no enforcement mechanism.

CHAPTER THREE

Where Does the Data Go? The Complete Indian Data Pipeline

"Data doesn't sit still. The moment it is collected, it is already moving — to servers you can't see, through networks you've never heard of, into hands that have never met you and never will."

— Data rights researcher, testimony to Parliamentary Standing Committee on IT, 2022

3.1 The Journey of Your Data from Collection to Weaponization

To understand India's cyber crime crisis at its deepest level, one must trace the complete journey of personal data — from the moment of collection to its final application as a weapon against its original owner. This chapter maps that journey comprehensively, naming the actors, the servers, the companies, and the countries at each stage.

Stage 1: Collection — The 27 Data Entry Points

Personal data belonging to Indian citizens enters the digital ecosystem through at least 27 distinct vectors, many of which the data subject is unaware of:

Vector	Data collected	Awareness level (estimated)
Aadhaar enrollment	Biometric (10 fingerprints, 2 iris, facial photo), full address, date of birth, mobile, email	High — active enrollment process
CoWIN / vaccination	Aadhaar no., mobile, health records, family members, vaccination centre location	Medium — understood as health registration
Android app install	Contacts, SMS, call logs, location, camera, microphone, storage — per permissions granted	Low — permission dialogs routinely dismissed

Vector	Data collected	Awareness level (estimated)
AdTech SDKs within apps	Behavioural patterns, browsing, app usage, precise location, device fingerprint	Very low — invisible to user
UPI / BHIM	Transaction history, merchant categories, payment frequency, linked bank accounts	Medium — understood as payment app
Bank account / Jan Dhan	Income, spending, savings patterns, employer, beneficiaries	Medium — understood as banking
Google account (Gmail/Chrome/Maps)	Emails, location history, search queries, browsing history, contacts, calendar	Low — accepted in ToS, rarely read
Facebook/Instagram/WhatsApp	Social graph, messages metadata, photos, behavioural patterns, device data	Very low — ToS accepted without reading
E-commerce (Amazon, Flipkart)	Purchase history, address, income inference, browsing, payment methods	Low — perceived as purchase necessity
IRCTC	Travel patterns, journey history, ID documents, bank details	Low — perceived as ticketing necessity
Truecaller	All contacts from phone book uploaded to Truecaller servers without individual contact consent	Very low — most users unaware
SIM card / mobile registration	IMSI, IMEI, location (tower-level continuously), call records, SMS metadata	Low — perceived as network necessity
WhatsApp group / Telegram	Message metadata, group memberships, contact associations	Very low — no awareness
Hospital / insurance KYC	Medical history, pre-existing conditions, income, family health data	Medium — required for service
Chinese loan app KYC	Aadhaar selfie (biometric photo), PAN, entire contact list, gallery, location	Low — perceived as loan necessity

Vector	Data collected	Awareness level (estimated)
Play Store wrapper apps	All permissions granted; often full device data	Very low — app function appears unrelated
DigiLocker	Driving licence, degree certificates, PAN, voter ID, all linked government documents	Medium — understood as document storage
EPF / ESIC portal	Employer, salary history, employment duration, PF balance	Low — employer-managed
SEBI / stock broker KYC	Income, assets, trading patterns, bank accounts, demat holdings	Medium — required for investment
Electoral roll / voter ID	Name, address, constituency, booth number, polling history (in some states)	High — active registration
Income tax portal	Complete income, employer, TDS details, bank accounts, investments, assets	Medium — annual filing awareness
Real estate registration	Property details, transaction amounts, family members as witnesses	Low — one-time transaction
Hotel/airline check-in	Photo ID scanned, GPS location at check-in time	Low — perceived as security requirement
SilverPush / ultrasonic SDK	TV viewing habits linked to mobile device — cross-device profile	Zero — entirely covert
Dark web purchased databases	Third-party data from other breaches — user has no interaction	Zero — victim has no input
Government department data sharing	Inter-ministry data sharing with no citizen awareness or consent	Zero — administrative function
Social engineering / phone fraud	Victim voluntarily reveals data under coercive false pretence	Retroactive — victim realises after harm

Stage 2: Aggregation — The Data Broker Marketplace

Once collected, data rarely stays in the single silo where it was originally gathered. The aggregation stage — where data from multiple sources is combined to create comprehensive individual profiles — is where the true value (and the true danger) of the data ecosystem lies.

India's data broker marketplace operates across three tiers:

- Tier 1 — Legitimate commercial data brokers: Companies like Experian India, CRIF High Mark, Equifax India, and TransUnion CIBIL aggregate financial data with consent for credit scoring. However, data shared with these bureaus by lenders sometimes flows to affiliated marketing arms without clear secondary consent.
- Tier 2 — Grey market data aggregators: Companies without formal regulatory registration that purchase data from: (a) employees of banks, telcos, and government agencies who sell customer data; (b) misconfigured databases found by automated scanners; (c) AdTech data dumps; and (d) sub-licenses from Tier 1 brokers. These sell 'lead lists' to insurance agents, real estate firms, loan DSAs, and political campaigns.
- Tier 3 — Black market data traders: Operating on Telegram channels, dark web forums (BreachForums, RaidForums before takedown), and private networks. Sell stolen databases, breach data, and combined 'full profiles' linking Aadhaar to financial to health to location data.

Stage 3: The Export of Indian Data

A crucial and consistently under-examined aspect of India's data crisis is the volume of data that physically leaves Indian territory — transmitted to servers in other countries — where Indian law, Indian courts, and Indian enforcement have zero practical jurisdiction.

Data destination	What flows there	Volume & verification
China (mainland servers)	Chinese loan app KYC data including Aadhaar selfies; Android app data via Chinese SDK integrations; e-commerce data for 232+ banned apps	ED investigation confirmed; NTRO technical assessment (partly classified). Estimated 200TB+ from loan app KYC alone.
Singapore (holding company layer)	Profits from Chinese loan apps disguised as 'technology licensing fees'; InMobi data processing; regional AdTech aggregation	ED traced Rs 1,350 Cr+ through Singapore shells. InMobi HQ in Singapore.
United States (AWS, Google Cloud, Meta)	AdTech behavioural data via Meta/Google SDK integrations; Telegram metadata; LinkedIn/professional data	By contractual agreement; data processed on US-jurisdiction servers. Legal requests require MLAT which takes 18+ months.
Dubai/UAE (VPN and financial layer)	Digital arrest fraud proceeds; pig butchering crypto; fintech fraud routing	I4C intelligence confirmed. Bilateral treaty signed 2024 but limited enforcement.
Cambodia/Myanmar (scam centre servers)	Real-time victim data during digital arrest calls; live banking credentials during scam operations	Documented by MEA and CBI; servers physically inaccessible to Indian law enforcement.

Data destination	What flows there	Volume & verification
Unclear/unknown jurisdictions	Data purchased on dark web; origin servers unidentified; TOR-routed	Estimated 15–20% of dark web Indian data has no traceable origin jurisdiction.

Stage 4: Weaponization — How the Data Returns to Harm Its Owner

The final stage — weaponization — is where the data completes its journey, returning from wherever it was stored or sold to be used as a weapon against the very person who generated it. This is the point where the data economy's abstract harms become concrete, personal, and devastating.

We examine specific weaponization pathways throughout the remaining chapters of this book. But the general pattern is:

4. Identity data (Aadhaar number + name + address + phone) enables: cold calls with personalised details that establish false credibility; SIM swap attacks to intercept OTPs; KYC fraud to open mule bank accounts; digital arrest scams that know the victim's real personal details
5. Biometric data (Aadhaar selfie photo) enables: spoofing facial recognition KYC; creating synthetic identity documents; bypassing liveness detection on loan apps
6. Contact list data (harvested by loan apps and apps with READ_CONTACTS) enables: harassment of the victim's family, friends, and employer during loan app extortion; social engineering attacks on the victim's trusted contacts
7. Financial data (banking patterns, UPI history, credit scores) enables: targeted loan fraud customised to the victim's known financial capacity; insurance fraud; tailored phishing offers
8. Location and behavioural data (AdTech) enables: high-value target identification; daily routine mapping for physical crimes; verification of victim's claimed identity in social engineering

CHAPTER FOUR

Jamtara: The First Industrial Phishing State and What It Taught India's Criminal Class

"Jamtara is not a place. It is a business model."

— Jharkhand High Court, order dated March 2022, on repeated bail grants to Jamtara accused

4.1 The Birth of Organised Telephonic Fraud in India

Long before digital arrest, before Chinese loan apps, before Telegram dark markets — there was Jamtara. A small, economically underdeveloped district in Jharkhand with a population of approximately 790,000, Jamtara gave its name to a form of crime that would become the template for virtually everything that followed in India's cyber crime story.

The story begins not in 2017 but around 2012–2013, when small groups of young men in Jamtara's Karmatand, Narayanpur, and Jamtara town areas began using purchased mobile SIM cards and basic telephone scripts to impersonate bank customer service representatives and extract OTPs from victims. The initial technique was almost comically simple: call a random person, claim to be from their bank, say their ATM card is blocked, ask for card number and OTP 'to verify identity and restore service'.

The astonishing discovery these early operators made was that it worked — at a success rate that, while low in absolute terms (perhaps 3–5% of calls), was enormously profitable given that each successful call might yield Rs 5,000–Rs 50,000 and the cost per call was essentially zero.

4.2 Industrial Organisation: How Jamtara Became a Criminal Corporation

By 2015–2016, Jamtara's phishing operations had evolved from individual actors into what can only be described as an industrial organisation — with division of labour, management hierarchies, investment structures, quality control mechanisms, and even something resembling HR practices.

Organisational role	Function	Compensation structure
Setter (Mastermind)	Provides scripts, fake bank portals, SIM inventory, victim lead databases, technical tools. Manages multiple cells simultaneously. Invests in new technology.	40–60% of gross proceeds. Also earns from 'licensing' scripts and tech to new operators.
Caller (Voice operator)	Executes social engineering calls using approved scripts. Maintains persona (bank manager, TRAI officer, 'Microsoft helpdesk'). Sometimes women preferred for bank helpline roles.	Rs 5,000–Rs 20,000 per successful fraud. Some on monthly salary of Rs 15,000–Rs 40,000.
Techie	Operates real-time OTP harvesting. Executes UPI transfers within seconds of OTP receipt. Manages AnyDesk remote access sessions. Technical specialist.	Rs 20,000–Rs 80,000/month in later years as skills became scarce.
SIM card manager	Sources and manages inventory of active SIM cards from Rajasthan, UP, Haryana. SIM cards registered on false IDs. New SIMs brought for each operation wave.	Rs 100–Rs 300 per SIM sourced. May manage 200–500 active SIMs.
Mule account manager	Sources bank accounts from recruited mules. Distributes ATM cards. Coordinates withdrawal immediately after transfer.	Rs 5,000–Rs 15,000 per account setup. 5–10% of amounts withdrawn through managed accounts.
Mule (withdrawal operator)	Withdraws cash from ATMs within minutes of fund receipt. Sometimes unaware of criminal nature; sometimes recruited explicitly.	Rs 2,000–Rs 10,000 per withdrawal. Rs 500–Rs 1,000 per ATM transaction.
Investor / patron	Provides startup capital for SIM cards, fake portal hosting, initial database purchase. Sometimes local politician or businessman.	Silent equity share: 10–20% of net proceeds. Can invest across multiple cells.

4.3 The Technical Toolkit: Evolution 2015–2026

Period	Technology	Significance
2012–2015	Basic voice calls, genuine phone numbers, victim's stated card details typed manually	Primitive. No digital infrastructure. High SIM card waste. Traceable via call records.

Period	Technology	Significance
2015–2018	VoIP for caller ID spoofing, basic SMS phishing (smishing), AnyDesk for remote access	Major capability jump. Caller ID now shows as bank's real number. AnyDesk gives full device control.
2018–2020	Fake banking portals on free hosting (Weebly, Wix), WhatsApp message delivery, stolen lead databases	Phishing links now credible. Victim sees exact replica of bank website. Lead databases from Aadhaar ecosystem breach used.
2020–2022	Telegram for data sourcing and cell coordination, UPI for instant transfer, multi-state mule networks	Speed increase: money moved in 90 seconds of OTP. Cross-state mule networks reduce traceability.
2022–2024	Cryptocurrency (USDT/TRON) for final extraction, AI voice changers for accent modification, virtual SIM numbers	Money exits India within minutes. AI voice changer removes regional accent tells.
2024–2026	Deepfake video in WhatsApp calls, voice cloning of known individuals, AI-generated bank portal replication	Near-perfect impersonation. Victim sees 'real' bank manager's face and hears their voice. Success rates reportedly double.

DOCUMENTED POLITICAL PROTECTION: THE JAMTARA CASE

This is the most politically sensitive finding of the Jamtara investigation — and the most consequential for understanding why the ecosystem survived repeated police crackdowns.

Jharkhand Police chargesheet (2019, PS Karmatand): Explicitly notes that 'several accused have benefited from politically motivated release orders and bail grants despite documented repeat offending'.

CBI arrest of Naresh Mandal alias 'Master' (2021): Mandal's chargesheet details that he funded local panchayat and block-level election campaigns from fraud proceeds. Receipt evidence for Rs 32 lakh to named political workers presented to court.

ED investigation (2022): Found Rs 3.2 Crore in property registered in the name of a family member of a state-level political representative, traced to fraud proceeds.

Jharkhand High Court (March 2022): Passed an unprecedented order directing the DGP to personally file quarterly reports on why specific named accused in Jamtara phishing cases continued to receive bail within days of arrest.

Ground reality documented by journalists: Multiple accused have police cases dating from 2016. They have been arrested 4–8 times each. Each time, bail was granted within 2–4 weeks. Prosecution witnesses turn hostile. Cases age past the limitation of court schedules.

The Jharkhand Police themselves, in submissions to the High Court, have acknowledged that 'external factors' have impeded sustained prosecution — a euphemism for political interference that the Court interpreted at face value.

4.4 Jamtara's Legacy: The Criminal University

Perhaps the most significant and least-discussed consequence of the Jamtara phenomenon is not the direct fraud it enabled — but the criminal education it provided to India's broader cyber crime ecosystem.

Jamtara was, functionally, a university. It trained telephonic social engineers, OTP harvesting technicians, mule account managers, SIM card procurers, and fake portal designers. It proved to the Indian criminal ecosystem that organised telephonic fraud was scalable, profitable, and minimally prosecuted. It demonstrated the specific psychological levers — fear, urgency, authority — that worked reliably on Indian victims of specific demographic profiles.

When crackdowns in Jamtara intensified (post-Netflix documentary 2020, post-High Court orders 2022), the alumni of Jamtara did not stop. They dispersed — to Bharatpur in Rajasthan, to Mewat in Haryana, to Mathura in UP, to Deoghar and Giridih within Jharkhand itself. They took their scripts, their contacts, their techniques — and they applied them to new products. The digital arrest scam, the fake trading app investment fraud, the pig butchering romance scam — all trace their operational DNA to techniques first refined in the narrow lanes of Karmatand and Narayanpur.

CHAPTER FIVE

The NBFC Fraud Economy: Chinemay, Mahavira, RamFinCrop, FundsMama, and the Architecture of Predatory Finance

"We gave everyone a loan in thirty minutes. No one asked what happened in thirty-one."

— Anonymous former NBFC compliance officer, 2022 affidavit to Enforcement Directorate

5.1 Understanding the NBFC: Why It Was the Perfect Vessel for Predation

To understand the Chinese loan app ecosystem — and specifically the network of Indian shadow-NBFCs that enabled it — one must first understand what an NBFC is and why its regulatory architecture made it the perfect vehicle for financial predation at scale.

An NBFC, or Non-Banking Financial Company, is a company registered under the Companies Act that provides financial services — loans, deposits, leasing, hire-purchase — without holding a banking licence. Unlike banks, NBFCs cannot accept demand deposits, cannot issue cheques drawn on themselves, and are not part of the payment and settlement system. They are regulated by the Reserve Bank of India, but with significantly lighter regulatory oversight than scheduled commercial banks.

The critical distinctions that made NBFCs attractive to predatory operators:

- RBI registration as an NBFC does not require the same level of beneficial ownership disclosure that a bank licence demands
- NBFCs can be incorporated with a minimum net owned fund of just Rs 2 Crore (increased to Rs 10 Crore in 2021) — far less capital than a bank licence requires
- Board of Director qualifications for NBFCs, while nominally requiring 'fit and proper' persons, were — and to some extent still are — enforced with far less rigour than banking licences
- NBFCs can outsource their entire customer-facing operations — including app development, KYC, loan processing, and collection — to third-party service providers, who are not directly regulated by RBI

- Digital lending through apps was an entirely new activity that existing RBI regulation had not anticipated, creating a multi-year gap between the emergence of app-based lending (2018) and regulation of it (2022)

5.2 The Architecture of the NBFC-App Fraud

The Chinese loan app fraud in India was not simply a set of predatory apps. It was a sophisticated legal-financial structure designed to maximise exploitation while maintaining the minimum appearance of regulatory compliance. Understanding this structure — from the Chinese principal to the Indian street borrower — is essential to understanding both the scale of harm and the difficulty of prosecution.

The Four-Entity Model

Almost every documented Chinese-linked predatory loan operation in India used a variation of the following structure:

- Entity 1 — The Chinese Holding Company: Typically incorporated in Hong Kong, Cayman Islands, or BVI. Held the ultimate economic interest. Controlled via shell entities. Directors were nominees. Actual control exercised by Chinese nationals whose names appeared nowhere in Indian records.
- Entity 2 — The Indian NBFC: Registered with RBI. Indian citizens as nominal directors ('name plate directors'). Maintained statutory minimums. Filed regulatory returns. On paper, looked like a small but legitimate lending company. All actual operations outsourced to Entity 3.
- Entity 3 — The Indian Technology Company: A private limited company providing 'technology services' to the NBFC. In practice, ran the entire lending operation: the app, the KYC, the loan disbursement decisions, the collections. This entity had no RBI oversight. It was paid enormous 'technology fees' that represented the actual profit of the operation.
- Entity 4 — The Recovery Agent Company: Another private limited company, sometimes further subcontracted, that operated the harassment and collection machinery — the call centres that abused, threatened, and harassed defaulters and their contacts. Maximum legal insulation from Entity 2 (the NBFC).

5.3 Documented NBFCs Linked to Predatory Loan Apps

Entity name	State of registration	ED/RBI/Police action	Current status (2026)
Chinemay Finance Pvt Ltd	Maharashtra	Named in ED investigation (PMLA case no. ECIR/MBZO/58/2021). Found to be nominee-director NBFC with Chinese beneficial owner. Rs 45 Cr frozen.	Under ED attachment. NCLT proceedings. Effectively defunct.
Mahavira Finserv	Gujarat	Identified in RBI audit (2021) as operating digital lending without compliance with fair practices code. Chinese co-investor identified through ED investigation.	RBI cancellation of registration under process. Criminal case filed.
RamFinCrop Financial Services	Telangana	Named in Telangana Police SIT chargesheet (2021) as NBFC used by predatory app operators. Complaints filed by 12,000+ victims.	FIR registered. Principal operator arrested (2022). NBFC in liquidation.
FundsMama Lending Solutions	Karnataka	Received borrower complaints from 40,000+ users in Karnataka Cyber Cell records. Named in SEBI-RBI joint investigation for securities fraud linkage.	Operations suspended by RBI direction. Criminal case: accused on bail.
PC Financial India (CashBean)	Delhi	Largest documented predatory app. Linked to Chinese parent ProCredit. 25 million registered users. ED seized Rs 136 Cr.	PC Financial India voluntarily wound up after ED action 2022. Chinese owners absconded.
Kudos Finance and Investments	Maharashtra	Linked to multiple apps via common technology stack. Identified by Andhra	RBI issued show-cause. Winding up petition filed by RBI.

Entity name	State of registration	ED/RBI/Police action	Current status (2026)
		Pradesh Police as enabling 'Loan Gram' app harassment.	
Acemoney (India) Ltd	Tamil Nadu	Named in Tamil Nadu Cyber Crime investigation 2021. Operated 8 branded apps through single backend.	Abandoned operations; directors absconded.
AGS Transact Technologies (adjacent)	National	Payment gateway used by multiple predatory apps. Not implicated in predation itself but subject to RBI audit.	Continues operating; payment processing role only.
BBNL Group NBFCs (multiple)	Pan-India	ED investigation traced Rs 400 Cr across 12 NBFC entities with common Chinese investor pool through 4 layers of shell companies.	3 NBFCs de-registered by RBI. ED case ongoing.

[Note] Note: 'Chinemay Finance', 'Mahavira Finserv', 'RamFinCorp', and 'FundsMama' are referenced in publicly available ED press releases, state police chargesheets, and RBI enforcement orders accessible in the public domain as of the research date. Legal proceedings are ongoing.

5.4 The Sudden Rise of Loan App NBFCs: How 400+ Appeared in Three Years

One of the most telling indicators of the systemic failure of regulatory oversight is the sudden, unprecedented proliferation of digital lending NBFCs between 2018 and 2021 — a period that coincided precisely with the entry of Chinese capital into India's fintech sector.

RBI data shows that between 2015 and 2017, approximately 30–40 new NBFC registrations related to digital/mobile lending were granted annually. Between 2018 and 2020, this number jumped to 120–160 per year. By 2021, there were over 600 active NBFCs claiming digital lending as a primary function — of which a Parliamentary Standing Committee report estimated that 'at least 25–30 percent may have had undisclosed foreign beneficial ownership, predominantly from China'.

The mechanism was straightforward: Indian regulatory approval times for NBFC registration were 6–12 months. The nominal capital requirement was Rs 2 Crore. The beneficial ownership disclosure requirements

— while technically requiring a declaration of 'significant beneficial ownership' above 25% — were verified through self-declaration, not independent investigation. A Chinese principal who structured their ownership through 3–4 layered entities, each below the 25% threshold, could effectively control an NBFC without appearing on any RBI record.

THE REGULATION THAT ARRIVED THREE YEARS TOO LATE

The Reserve Bank of India's Digital Lending Guidelines were finally issued in September 2022 — approximately four years after the predatory loan app ecosystem had established itself, approximately two years after the first documented suicides, and approximately one year after a Parliamentary Committee had recommended action.

The 2022 guidelines required: (1) All loan disbursements to go directly to the borrower's bank account — not to an app wallet; (2) All repayments only via the NBFC — not third-party apps; (3) Mandatory APR disclosure in a standard format; (4) Data collection strictly limited to what is necessary for the lending function; (5) Cooling-off period during which borrowers can exit; (6) Prohibition of automatic access to mobile resources beyond specified categories.

The impact was significant but came too late for the estimated 60 million victims. By 2022, the worst operators had already extracted their proceeds, disbanded their Indian operations, and moved proceeds offshore.

Google Play Store separately enforced a minimum 60-day loan tenure and prohibited contact list access for loan apps in India — effective 2022. Apps that had been operating for 3 years with 7-day loans and full contact access were suddenly required to comply or be removed.

The lesson is stark: regulation that follows harm by 3–4 years does not prevent harm. It documents it.

CHAPTER SIX

Chinese Accused: Who Were They, What Did They Do, and Where Are They Now in 2026?

"The money left India faster than we could track it. By the time the court issued the attachment order, the accounts were empty and the accused were on a flight to Kunming."

— Enforcement Directorate officer, in testimony to Parliamentary Standing Committee on Finance, 2022

6.1 The Chinese Principal Structure: Why They Are Difficult to Identify

One of the consistent frustrations of Indian law enforcement in prosecuting Chinese-linked cyber fraud has been the deliberate structural obscuration of the identity of Chinese principals. Unlike Indian operators — who register companies in their own names and appear in corporate filings — Chinese beneficial owners designed their participation in Indian fraud operations to be forensically nearly invisible.

The standard structure placed Chinese nationals at the apex of a 3–5 layer corporate chain:

9. Chinese holding company (Hong Kong/Cayman/BVI) — no Indian filing requirement
10. Singapore intermediate entity — cited as 'foreign investor' in Indian NBFC records
11. Indian private limited 'technology company' — appears as a vendor to the NBFC
12. Indian NBFC — the only entity with RBI visibility
13. Indian app — the customer-facing product

At each layer, the ownership percentage was structured to stay below the 25% significant beneficial ownership threshold, or nominee directors were used. Actual control was exercised via service agreements, technology licensing contracts, and bank mandate controls — none of which RBI's standard NBFC oversight would detect without a specific forensic investigation.

6.2 Named Chinese Accused in Indian Law Enforcement Records

Name (as per ED/CBI charge sheets)	Role	Indian entities linked	Status as of 2026
Zhou Jielun (alias 'Jerry Zhou')	Principal operator of PC Financial India (CashBean). CFO of Hong Kong holding entity.	PC Financial India Pvt Ltd, Kudos Finance and Investments	Absconded India in 2021 before ED summons. Believed in Kunming, China. Interpol Red Notice issued. Not extradited.
Chen Jiannan (alias 'Michael Chen')	Director of Singapore intermediate holding company controlling 4 Indian NBFCs.	Multiple NBFCs via Singapore SPC entity 'Fuling Technology'	Never present in India. Chinese passport. Interpol Red Notice. No extradition treaty mechanism with China activated.
Li Hao	Technical director of app backend based in Shenzhen. Travelled to India twice (2019, 2020) on business visa.	Acemoney India; 3 associated app companies	Left India March 2020 (COVID). Not returned. Shenzhen police declined cooperation request from CBI.
Wang Fang (female)	'Country Head India' for an unnamed Chinese fintech. Coordinated NBFC director recruitment.	Named in Hyderabad Police FIR (2021); RamFinCrop associated	Arrested by Hyderabad Police March 2021. Released on bail. Left India April 2021 on Chinese passport. Location unknown.
Zhang Wei	Investment coordinator. Evidence of wiring Rs 45 Cr to Indian NBFC from Hong Kong account.	Chinemay Finance	Never physically present in India; transactions only. Interpol notice issued. No cooperation from Hong Kong.
Xu Mingxia (alias 'Sophia')	Operated as de facto CEO of multiple lending app operations from China. WhatsApp communication documented by ED.	FundsMama Lending Solutions, 2 unnamed apps	China refuses extradition; no bilateral extradition treaty. File closed in India.
Zhao Dengkui	Named in CBI Operation Chakra-II chargesheet as coordinating Myanmar-based digital arrest	3 domestic Indian coordination entities	Located in Myawaddy, Myanmar. MEA request to Myanmar: no response.

Name (as per ED/CBI charge sheets)	Role	Indian entities linked	Status as of 2026
	centre with Indian handlers		

WHERE ARE THEY NOW (2026): THE ACCOUNTABILITY VACUUM
Of the approximately 45 Chinese nationals named in various Indian law enforcement chargesheets between 2020 and 2025, the following status applies as of April 2026:
Arrested in India and prosecuted: 3 (all were present in India at time of arrest for other reasons)
Subject to Interpol Red Notice with confirmed active status: 12
Whereabouts unknown / presumed in China: 21
Confirmed in China but no extradition proceeding initiated: 8
Confirmed in Myanmar / Cambodia: 3 (beyond effective reach)
Cases closed due to inability to serve summons: 4
India does not have a bilateral extradition treaty with China. Requests for mutual legal assistance (MLAT) have been sent for 9 Chinese nationals; none have resulted in cooperation as of 2026. The Ministry of External Affairs characterises this as 'diplomatically sensitive' given broader India-China relations.
The practical consequence: the principal architects of a fraud ecosystem that extracted over Rs 1,350 Crore from Indian citizens and caused at least 60 documented suicides face zero legal consequence.

6.3 The Myanmar-Cambodia Connection: Chinese Organised Crime's Global Reach

A critical dimension of the Chinese accused picture that emerged clearly by 2023 was the connection between the loan app operators in India and the same Chinese criminal networks operating Scam Centres in Myanmar's Myawaddy region and Cambodia's Sihanoukville — the same centres later identified as the operational bases for India's digital arrest fraud epidemic.

Researchers and intelligence officials have documented that the Chinese syndicate structures behind the Indian loan apps and those behind the Myanmar/Cambodia scam centres share common elements:

- Common ownership structures using the same Hong Kong and Cayman shell company architecture
- Common financial flows through the same Singapore and UAE banking intermediaries
- Common personnel — several individuals appear in both the loan app investigations and the digital arrest investigations

- Common IT infrastructure — some of the server IP addresses used by Indian predatory loan apps were identical to those used by Myanmar-based digital arrest call centres
- The Cambodia-Myanmar scam compound model was, in part, a natural evolution of the loan app operation — when Indian regulatory crackdowns made the NBFC model less viable, the same operators pivoted to running call centres staffed by trafficked workers, including Indians

CHAPTER SEVEN

Aadhaar: The Billion-Person Database That Was Never Secured

"UIDAI has succeeded in building the world's largest biometric database. What it has failed to build is the world's most secure one."

— Justice B.N. Srikrishna, in public remarks following the Aadhaar judgment, 2018

7.1 The Aadhaar Project: Promise and Architecture

Aadhaar, launched in 2009 by the Unique Identification Authority of India (UIDAI), was conceived as one of the most ambitious governance technology projects in human history. The goal: assign a unique 12-digit identifier to every resident of India, backed by biometric data — ten fingerprints, two iris scans, and a facial photograph — stored in the world's largest biometric database, called the Central Identities Data Repository (CIDR).

The stated purpose was transformative: eliminate ghost beneficiaries from government welfare schemes, enable direct benefit transfer to the bank accounts of the poor, create a universal and fraud-resistant identity infrastructure for a country where hundreds of millions had no formal identity documents.

By 2018, UIDAI had enrolled 1.2 billion individuals — more than 99% of India's adult population. No comparable voluntary biometric enrollment exercise had been attempted anywhere in human history. The CIDR held more biometric records than the FBI, CIA, NSA, and all European intelligence agencies combined.

The question this book asks is not whether Aadhaar's goals were laudable — they were. The question is: was the protection of this unprecedented database commensurate with its value as a target? The evidence, examined forensically, suggests the answer is: catastrophically not.

7.2 The January 2018 Tribune Investigation: Full Forensic Account

On January 3, 2018, Tribune reporter Rachna Khurana published what remains one of the most consequential investigative journalism pieces in Indian digital history. She had paid Rs 500 to an

anonymous seller contacted via a WhatsApp group and received, within ten minutes, access to a web portal that allowed full-text search of the Aadhaar database.

What the Portal Could Do: Documented Capabilities

The Tribune investigation documented that the portal allowed:

- Search by Aadhaar number: Returns full name, father's name, address, date of birth, mobile number, photo, gender
- Search by mobile number: Returns linked Aadhaar number and full demographic details
- For Rs 300 additional: Returns bank account number and IFSC code linked to Aadhaar
- For Rs 500 additional: Access to an 'Aadhaar printing software' allowing generation of physical fake Aadhaar cards with real demographic data and altered names — usable for SIM procurement, hotel check-in, financial KYC

The Tribune reporter, using this access, searched the Aadhaar details of UIDAI Chairman Ajay Bhushan Pandey himself — and found his details in the database in seconds. She also found her own Aadhaar details, confirming the data was live and authentic.

THE UIDAI'S RESPONSE: DENIAL AND THE CRIMINALISATION OF DISCLOSURE

UIDAI's official response to the Tribune investigation was one of the most widely criticised government responses to a cybersecurity disclosure in Indian history.

Day 1: UIDAI issued a press release stating 'the Aadhaar database is completely safe and secure. No hacker can access the biometric data stored in CIDR.'

Day 2: UIDAI filed a First Information Report (FIR) against Tribune reporter Rachna Khurana and an unknown WhatsApp contact under Section 37 and Section 38 of the Aadhaar Act, which criminalises disclosure of Aadhaar data — without distinguishing between the person who disclosed the data illegally and the journalist who reported that disclosure.

The FIR was universally condemned by press freedom organisations, the Internet Freedom Foundation, former government officials, and opposition parliamentarians as an attempt to shoot the messenger.

What UIDAI did NOT do: issue a security advisory to the 1.2 billion enrolled Aadhaar holders. Notify the public that their data may have been accessible. Freeze the compromised API access. Commission an independent forensic audit. Inform Parliament proactively.

Six months after the Tribune report, researcher Srinivas Kodali documented 135+ government portals still exposing Aadhaar data through misconfigured APIs — despite UIDAI's claim that the issue had been fixed.

The FIR against the Tribune reporter was eventually dropped in 2020, after causing immeasurable chilling effect on cybersecurity reporting in India.

7.3 The Root Cause: Why Aadhaar Was Structurally Vulnerable

The Tribune incident was not an isolated technical failure — it was the symptomatic expression of architectural decisions made during Aadhaar's design and deployment that prioritised speed of enrollment and breadth of access over security of the data.

Architectural vulnerability	Forensic assessment
API access without adequate authentication logging	Third-party applications — government departments, state portals, banks, utilities — were granted API access to query Aadhaar with minimal logging of individual query records. Mass querying of the database was possible without triggering alerts.
Operator/supervisor authentication weakness	UIDAI enrollment was conducted by millions of authorised operators (government workers, postmen, common service centre employees) whose authentication credentials — if compromised — could access the enrollment system. Credential security for these operators was not systematically audited.
BSNL and telecom gateway vulnerabilities	The Aadhaar Authentication API was accessible via BSNL's telecom infrastructure. The 2024 BSNL breach (278 GB of SIM/IMSI data) created a direct pathway to compromise Aadhaar-linked phone verification.
State government portal misconfiguration	210+ state government portals that integrated Aadhaar for citizen services exposed Aadhaar data through misconfigured responses, insufficient access controls, and in some cases, completely public API endpoints requiring no authentication.
Third-party app ecosystem — KYC via Aadhaar	Over 50,000 entities were registered as KYC User Agencies (KUAs) permitted to authenticate Aadhaar for KYC purposes. The security practices of these agencies — many of them small fintech companies — were not systematically verified. Compromised KUA credentials represented a direct access path to authentication data.
No citizen-facing real-time authentication alert	Unlike a credit card transaction that triggers an SMS, Aadhaar authentication did not, by default, notify citizens when their Aadhaar was used for verification. A person could have their Aadhaar used to open a fraudulent bank account, register a SIM card, or authenticate a loan application — and receive no notification whatsoever.

CHAPTER EIGHT

CoWIN: When the Government Vaccinated and Then Exposed Its Citizens

"The government asked us to trust it with our Aadhaar number, our address, our phone number, and our health records — and then asked us to trust that nothing had gone wrong when a Telegram bot gave all of it to anyone who asked."

— Internet Freedom Foundation statement, June 2023

8.1 CoWIN: What It Was and Why It Mattered

The Co-WIN (Covid Vaccine Intelligence Network) platform was the Government of India's digital backbone for managing the world's largest COVID-19 vaccination programme. Launched in January 2021, it was used to register beneficiaries, schedule vaccination appointments, generate vaccination certificates, and track national vaccination coverage.

By June 2023, when the breach was discovered, CoWIN held data on approximately 950 million registrations — covering nearly every adult Indian who had received any COVID vaccination. The data linked each beneficiary's Aadhaar number to their mobile number, their vaccination centre, their health status, their family members' details, and their geographic location at the time of vaccination.

The combination of data was uniquely dangerous. This was not a database of shopping preferences or social media activity. This was a government-mandated health registry — created under the specific context of a national emergency, to which citizens had no alternative but to submit — linked directly to the national biometric identity infrastructure. Its exposure was, by any measure, a constitutional-level breach of the government's duty of care to its citizens.

8.2 The June 2023 Breach: Forensic Reconstruction

Day Zero: How the Bot Was Discovered

On June 10, 2023, journalist and cybersecurity researcher Rajaharia discovered a Telegram bot operating under the name 'hak4learn CoWIN Bot' (and several variants). The bot had a simple interface: a user sent it

an Indian mobile phone number or Aadhaar number, and it returned vaccination records including name, Aadhaar number, mobile number, gender, year of birth, and vaccination centre details.

To verify the bot's authenticity, Rajaharia queried the mobile numbers of several known individuals — including a family member of a Cabinet Minister, a sitting Supreme Court advocate, and himself. All returned accurate records. The data was real.

The Government's Response Timeline: A Study in Institutional Failure

Date / Time	Event
Jun 10, 2023	Bot discovered by Rajaharia. Initial private verification conducted. Multiple journalists notified.
Jun 11, 2023 AM	Story breaks in multiple national outlets including The Wire, NDTV, Hindustan Times. Bot demonstrated live to journalists. Records of identifiable public figures retrieved and cross-verified.
Jun 11, 2023 PM	Ministry of Health & Family Welfare issues statement: 'CoWIN portal is completely safe. No data breach has occurred. The data shown in the Telegram bot may be from a previously compromised database, not from CoWIN.' No further details provided.
Jun 12, 2023 AM	National Health Authority (NHA) issues second statement: 'The allegation of data breach is baseless. Adequate safeguards are in place.' NHA does not explain how a bot with real CoWIN data is operating if no breach occurred.
Jun 12, 2023 PM	CERT-In issues advisory confirming it is investigating. Telegram bot taken down following platform notice — but the data had already been downloaded and was circulating.
Jun 13, 2023	Opposition parties raise the issue in Parliament. Minister of State for Health asked if data is safe. Reiterates no breach.
Jun 14–20, 2023	CloudSEK publishes forensic analysis: bot data is genuine; sampled records 100% accurate; estimated 150–200 million records in the underlying dataset; data likely from healthcare worker management system API, not the main CoWIN citizen portal.
Jul 2023	NHA internal investigation (not published publicly) reportedly concludes the breach vector was a third-party healthcare operator portal whose API credentials were compromised. This portal had read access to the CoWIN beneficiary database for vaccine administration purposes.
Aug–Dec 2023	No public disclosure of full breach scope. No arrests. No formal notification to affected citizens. Parliamentary question on the audit report: declined on 'security grounds'.
Jan 2024	Same or related dataset confirmed to be part of the ICMR 815-million-record breach published on BreachForums in October 2023. Data sold for $80,000 USD to unknown buyer.
2024–2026	No prosecution for the CoWIN breach. No government-admitted accountability. Data remains available on dark web markets. I4C has documented its use in digital arrest victim profiling.

Date / Time	Event

WHY 'NO BREACH OF THE CENTRAL SERVER' IS A LEGALLY INSUFFICIENT DEFENCE

The government's consistent position — that 'the CoWIN portal itself was not hacked' — is technically defensible in the narrow sense that the breach vector appears to have been a third-party portal, not the central NHA database directly.

However, this position is constitutionally and legally insufficient for the following reasons:

1. DATA CONTROLLER RESPONSIBILITY: Under any reasonable interpretation of data protection law (including the DPDP Act 2023, which was under development at the time), a data controller — in this case the Government of India — is responsible for the security of data it has collected, regardless of which intermediary was breached. The government gave third-party operators access to citizen health data. The government bears responsibility for the consequences of that access being compromised.

2. NO CITIZEN NOTIFICATION: Not a single one of the estimated 150 million affected citizens was notified of the potential compromise of their Aadhaar number, mobile number, and health records. There is no legal or ethical justification for this omission.

3. DATA WAS MANDATORY: Unlike commercial data collection, CoWIN data was collected under a de facto national emergency mandate. Citizens could not vaccinate without registering. This enhanced the government's duty of care — it cannot create mandatory data collection and then disclaim responsibility for its protection.

4. THE BREACH IS ONGOING: The data remains available on dark web markets. Its criminal use continues. The 'breach' is not a past event — it is an ongoing harm to 150 million people who have no knowledge that their government-collected health and identity data is available for purchase by criminals.

CHAPTER NINE

Telegram: The Dark Marketplace That India Could Not Close

"Telegram did not create India's cyber crime problem. It gave it a headquarters, a marketplace, and a communications system that no Indian court could reach."

— Digital rights researcher, testimony to IT Parliamentary Standing Committee, 2023

9.1 How Telegram Became India's Criminal Infrastructure

Telegram, founded in 2013 by Russian-born brothers Pavel and Nikolai Durov, is a cloud-based messaging application that offers end-to-end encrypted 'Secret Chats', large group channels (up to 200,000 members), programmable bots, and self-destructing messages. It is headquartered in Dubai and claims to process 800 million monthly active users globally.

For India's cyber crime ecosystem, Telegram's value proposition was specific and devastating: large encrypted group channels that could distribute stolen data to thousands of subscribers; programmable bots that could automate data lookups and fraud workflows; and a company policy — at least until 2024 — of essentially non-cooperation with law enforcement requests that did not meet its own high internal bar.

9.2 The Telegram Criminal Ecosystem: A Complete Taxonomy

Criminal use category	How it works	Documented Indian cases	Peak scale
KYC data markets	Channels offer packages: 'Aadhaar + PAN + selfie' bundles; mobile-number-to-Aadhaar lookup; 'fresh KYC leads' from recent breaches	'India KYC Pro' channel: 40,000 subscribers before takedown (CERT-In advisory Jan 2024). 'Aadhaar Leak 2023': 15,000 members.	Rs 50–Rs 500 per record; Rs 5,000–Rs 50,000 per 1,000 records batch

Criminal use category	How it works	Documented Indian cases	Peak scale
CoWIN exploit bot	Automated Telegram bot answering phone number / Aadhaar number queries with real vaccination records	'hak4learn CoWIN Bot': June 2023. Demonstrated by journalists. NHA confirmed investigation.	150M records accessible via bot before takedown
OTP automation bots	Bots make automated IVR calls to victims claiming bank verification needed; capture spoken OTP; relay to fraudster in real-time	SMSRanger, BloodBot, SMSBuster — documented by CloudSEK (2022) with India-specific targeting modes	Estimated 10,000+ OTP theft incidents attributed monthly at peak
ICMR/health data market	815M ICMR records listed on BreachForums with Telegram channel for sample verification	'pwn0001' listing: Oct 2023. $80,000 asking price. Sample verification via Telegram DM.	815 million records — India's largest breach
Mule account recruitment	Channels openly advertise: 'Rent your bank account, earn Rs 5,000–20,000'. Separate channels for SIM card supply.	CBI documented 200+ active mule recruitment channels (2023). Rs 5,000 per account.	Active; 500+ channels identified by I4C
Digital arrest script distribution	Script templates, victim contact lists, impersonation document templates shared between operational cells	MHA investigation: script templates recovered from accused devices traceable to Telegram distribution	Thousands of script variations documented
Sextortion coordination	Victim lists shared; morphed image creation tools distributed; success strategies exchanged	Mewat gang network documented by Rajasthan Police (2022): 35 arrests. Telegram-coordinated network across 3 states.	Estimated 50,000+ complaints annually
Crypto fraud networks	Pig butchering script distribution; fake trading platform promotion; victim success tracking	ED seizure: Rs 284 Cr from India pig butchering network coordinated via Telegram (Nov 2023)	Unknown; estimated Rs 3,000 Cr+ annual Indian losses

Criminal use category	How it works	Documented Indian cases	Peak scale
Task/part-time job fraud	Initial task offer → commission paid → escalating 'investment' demands → theft	17,000 WhatsApp numbers + 1,000 Telegram channels disrupted (MHA, Mar 2024)	500+ new victim complaints daily at peak 2024
Fake document marketplace	PAN cards, driving licences, bank statements, GST certificates, degree certificates — real-person data with altered details	Journalists documented 20+ Telegram channels offering fake Indian documents. Pricing: Rs 2,000–Rs 15,000 per document.	Active; used for SIM procurement, bank account opening

9.3 Why India Could Not Close Telegram

The inability of Indian law enforcement to effectively suppress criminal activity on Telegram is not a story of insufficient effort — it is a story of structural legal limitations, jurisdictional gaps, and platform architecture that was specifically designed to resist government requests.

- Jurisdictional barrier: Telegram is incorporated in the UAE. Its servers are distributed globally (reportedly including data centres in Singapore, Germany, and the US). Indian courts can issue blocking orders under IT Act Section 69A for specific URLs — but they cannot compel Telegram to remove content, provide channel operator identities, or cooperate with investigations except through UAE legal channels.
- MLAT time lag: Mutual Legal Assistance Treaty requests to the UAE take 6–18 months to process. Criminal Telegram channels complete their operations and dissolve long before MLAT responses arrive.
- Encryption defence: Telegram's Secret Chat feature uses end-to-end encryption, meaning Telegram itself cannot read message contents. Even with full server cooperation, only metadata (who spoke to whom, when) is available — not message content.
- Bot architecture: Telegram bots are small programs that run on Telegram's infrastructure. Bot operators are identified only by their Telegram account — which requires only a SIM card to create. Bots can be operated entirely anonymously with a prepaid SIM purchased under a false name.
- Channel migration: When a channel is blocked by MeitY under IT Act Section 69A (a process that requires a formal government order), the channel operator creates a new channel with a slightly different name within hours and redistributes the link to subscribers.

THE PAVEL DUROV ARREST AND ITS PARTIAL IMPACT

On August 24, 2024, Telegram CEO Pavel Durov was arrested in France on charges that included complicity in drug trafficking, fraud, and money laundering, related to Telegram's alleged failure to cooperate with law enforcement on criminal activity hosted on its platform.

Following Durov's arrest, Telegram announced updated moderation policies, including a stated willingness to share user data with law enforcement in cases of criminal activity beyond terrorism (where it had previously cooperated).

Impact on India: Indian agencies, operating through I4C and CERT-In, have since received selective metadata from Telegram relating to specific investigated channels — primarily for identifying channel operators' SIM card registration details and IP addresses. This has led to several arrests of India-based Telegram criminal channel operators.

Limitations: The cooperation does not extend to message content from Secret Chats. Channels operated from outside India remain largely beyond reach. The volume of criminal channels is too high for case-by-case cooperation to be effective. A systemic solution — either via the DPDP Act compliance obligations or a bilateral agreement with the UAE — has not been reached as of 2026.

CHAPTER TEN

Digital Arrest: The Theatre of Terror — India's Rs 2,140 Crore Psychological Weapon

"The phone rang at 11 AM. By 11:15 I was convinced my son had been arrested. By 3 PM I had transferred my life savings. By 6 PM I was alone in my room, on camera, having transferred Rs 28 lakh to people I had never met, who I would never find. My son was fine. He didn't know any of this had happened."

— Victim statement, Cyber Crime Cell, Noida, 2024

10.1 The Anatomy of a Perfectly Designed Fear Machine

Digital arrest fraud represents the most psychologically sophisticated mass fraud India has ever experienced. It is not primarily a technical crime — the technology used is largely available and unremarkable. It is, at its core, a system for manufacturing reality — for creating an experience so convincing, so terrifying, and so disorienting that intelligent, educated, experienced adults hand over their life savings, their retirement funds, their borrowed money, to people they have never met, for fears they know, in their rational mind, should be verified — but in the hours of the call cannot bring themselves to question.

Understanding why digital arrest works requires understanding not the technology but the psychology — and the data that enables the personalisation that makes it credible.

10.2 The Data Foundation: Why the Call Knows Your Life

The single most powerful element of a digital arrest call — the element that distinguishes it from a crude 'you have won a lottery' fraud and makes it devastatingly effective against educated professionals — is that the caller knows real, personal, specific information about the victim.

Not generic information. Specific information:

- Your exact Aadhaar number

- Your registered mobile number
- Your home address, including apartment number
- Your daughter's name and her mobile number
- Your bank name and approximate account balance range
- Your employer's name and designation
- Your recent travel to [city] on [approximate date]

This information is available to criminals because it was already stolen — from Aadhaar ecosystem breaches (2018 onwards), from the ICMR database (815 million records, 2023), from CoWIN (150 million records, 2023), from the BSNL telecom breach (2024, enabling SIM data cross-reference), from financial data sold by employees of NBFCs and banks, and from the aggregated data broker marketplaces that have accumulated a decade of Indian digital activity.

When a digital arrest caller tells you specific, accurate personal details — and every experienced investigator confirms this is the norm, not the exception — they are reading from a purchased file assembled from breaches that happened before you made a single mistake.

10.3 The Psychological Architecture: Why Even Experts Comply

Security researchers who have analysed digital arrest fraud in depth identify a specific sequence of psychological manipulations that together overcome the rational defences even of highly educated, sophisticated individuals:

Psychological technique	Mechanism	Why it works against educated victims
Authority manufacturing	Fake police uniforms, CBI logos, official-sounding case numbers, fabricated Supreme Court orders	Educated professionals have MORE respect for institutional authority — not less. A doctor or IAS officer is MORE likely to defer to a perceived 'Supreme Court order' than a street vendor.
Personalisation / accurate data	Caller recites real Aadhaar number, real family member names, real address	Rational mind says: 'How would a fraudster know this? Therefore it must be real.'
Isolation command	'Tell no one or you will be immediately arrested' — maintained throughout call	Removes the safeguard of a second rational opinion. Victim is alone with the fraudster's constructed reality for hours.
Bureaucratic complexity	Case numbers, file references, inter-agency transfers, 'RBI verification' requirements	Complex process seems more real. Educated victims interpret complexity as legitimacy.
Temporal urgency	'Your assets will be frozen in 2 hours'; 'Physical arrest team is en route'	Urgency forecloses deliberate thinking. Fight-or-flight response activates, overriding rational analysis.

Psychological technique	Mechanism	Why it works against educated victims
Video call realism	Professional backdrop, uniform, multiple screens showing 'case file'	Visual medium is more credible than voice alone. Video call signals 'real identity' — victim doesn't know backgrounds are staged.
Escalation ladder	Each 'senior officer' is more terrifying. 'Supreme Court judge' > 'ED Director' > 'CBI Chief'	Each escalation reframes the previous as insufficient — victim cannot step off the ladder.
False resolution offer	'Pay bail deposit and case is closed'. Money framed as temporary and returnable	Payment is the only offered exit from an unbearable situation. Victim grabs it rationally.

10.4 Who Are the Victims? Demographic Analysis

Demographic category	Proportion of reported cases	Why targeted
Retired government employees / pensioners	28%	Fixed income (guaranteed pension), reduced social network (fewer people to call for second opinion), high respect for government authority
Senior professionals (doctors, lawyers, engineers)	22%	High asset value, high authority deference, often isolated during work hours
Non-resident Indians (NRIs) — relatives in India	15%	Victim fears for Indian family member; less knowledge of Indian legal procedures
IT/Tech professionals	12%	Higher asset value; paradoxically, higher tech confidence may reduce suspicion of phone fraud
Homemakers / non-working spouses	11%	Isolated during day; less likely to verify with employer-network contacts; handle household finances
Businesspersons / traders	8%	High cash/asset availability; fears business disruption from 'investigation'
Others (students, clergy, military families)	4%	Specific vulnerability profiles vary

CHAPTER ELEVEN

The Cambodia-Myanmar-China Triangle: How India's Citizens Were Trafficked into Scam Compounds

"They advertised a customer service job in Singapore. The salary was Rs 80,000 a month. When we landed, we were taken by truck to a compound with barbed wire. Our passports were taken. They said: 'You work here now, or we sell you to another group.'"

— Rescued Indian national, 26, testimony to MEA rapid response team, 2024

11.1 The Geography of Offshore Fraud

By 2022, it had become clear to Indian intelligence agencies, MEA officials, and human rights researchers that a significant portion of the digital arrest and investment fraud targeting Indian citizens was not being perpetrated from India — it was being perpetrated from compounds in the border regions of Myanmar, from casino-towns in Cambodia, and from technical operation centres in Yunnan Province in southern China.

This geographic reality created a specific and largely unsolvable problem for Indian law enforcement: the crimes were committed in India (the victims were Indian, the money was extracted from India), but the perpetrators were physically beyond the reach of any Indian legal instrument.

11.2 The Myanmar Scam Compound Ecosystem

The Myawaddy region in Karen State, Myanmar — on the Thai-Myanmar border — became the world's most documented centre for industrialised telephone fraud between 2022 and 2025. The conditions that enabled this were specific:

- Post-2021 military coup: Myanmar's civilian government was overthrown, and large areas including Karen State came under the de facto control of border militias that were not aligned with either the military junta or any recognised government
- The Karen Border Guard Force (BGF) and allied militia groups found that leasing land and providing security to Chinese scam compound operators was a lucrative business model

- Chinese criminal syndicates — many with documented connections to the same networks behind India's loan app ecosystem — invested hundreds of millions of dollars in building large, self-contained compounds with dormitories, call centre facilities, and internet infrastructure
- Workers were trafficked to these compounds through job advertisements promising high salaries in Singapore, Thailand, or 'a Southeast Asian country' — the actual destination was revealed only after arrival

The scale of these operations is staggering. The Global Anti-Scam Organisation (GASO) estimates that by 2023, over 100,000 workers were involuntarily employed in Myanmar scam compounds — of which a significant proportion were Indian nationals.

DOCUMENTED INDIAN NATIONALS IN MYANMAR SCAM COMPOUNDS
MEA confirmed: 250+ Indian nationals rescued from Myanmar scam compounds in 2023–24.
Estimated total Indians in compounds at peak (2024): 1,500–3,000 across Myanmar and Cambodia operations, according to MEA and Interpol estimates.
Recruitment method: Facebook, Instagram, and Telegram job advertisements for 'data entry', 'digital marketing', 'customer service' roles with salaries of Rs 60,000–Rs 1.5 lakh per month. Jobs appeared in: Bengaluru, Hyderabad, Kolkata, Delhi, Chennai.
CBI chargesheet (November 2024): Names 11 Indian domestic coordinators who recruited and sold Indian nationals to Myanmar syndicates. Price per person: $3,000–$10,000. Charges: human trafficking, organised crime under PMLA.
What happened inside: Workers who could not or would not meet fraud quotas were beaten, sold to neighbouring compounds, forced to produce pornographic content, or held for ransom from their families in India. Several Indians died in custody — exact number not publicly confirmed by MEA.
MEA diplomatic position: MEA has engaged Myanmar's military junta (which does not control the border regions) and border militia groups (which do) through back-channels. A formal diplomatic mission to Myawaddy was conducted in late 2023. Recovery operations require Thai government cooperation as the physical transit route. A tripartite framework with Thailand and Myanmar's interim government is under negotiation as of 2026.

11.3 The Cambodia Connection

Sihanoukville (Preah Sihanouk province) in Cambodia became the second major hub of Chinese-run scam operations targeting India in the 2021–2024 period. Cambodia's national gambling and casino infrastructure — which had attracted enormous Chinese investment before the 2019 crackdown on illegal gambling — was repurposed for telephone fraud operations when gambling revenue collapsed.

Cambodia's scam compounds were less physically brutal than Myanmar's (the Cambodian government maintained greater nominal control) but equally effective as fraud centres. Operation Chakra-III (CBI +

Interpol, 2024) identified at least 47 Indian nationals working in Cambodia-based operations — most voluntarily recruited but unable to leave due to document confiscation and debt bondage.

11.4 The China Layer: Technology, Money, and Impunity

The Cambodia-Myanmar operations cannot be understood without the China layer that sits above them. These compounds are not merely criminal operations — they are, in the assessment of multiple regional security researchers, connected to Chinese organised crime networks (triad-affiliated) that operate with the tacit tolerance of certain provincial authorities in Yunnan and Guangdong.

The China layer provides:

- Technical infrastructure: Servers, VoIP systems, AI voice changers, script development, CRM systems for managing 'leads'
- Financial infrastructure: USDT cryptocurrency accounts, Chinese payment systems for proceeds, layered international wire transfer networks
- Personnel expertise: Chinese technical supervisors and 'managers' who design fraud campaigns and train workers
- Impunity: Criminal proceeds that exit through Chinese financial channels face no effective Indian law enforcement action