INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 5 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CALL CENTER-BASED SCAM OPERATIONS: INVESTIGATING CYBER FRAUD NETWORKS

AUTHOR - MUKUL TARE & PRATHMESH NAIK,

2ND YEAR BALLB STUDENTS AT KES SHRI JAYANTILAL H. PATEL LAW COLLEGE

BEST CITATION – MUKUL TARE & PRATHMESH NAIK, CALL CENTER-BASED SCAM OPERATIONS: INVESTIGATING CYBER FRAUD NETWORKS, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (5) OF 2026, PG. 54-61, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The rapid growth of digital communication and global connectivity has significantly changed the nature of crime, leading to the rise of complex cyber frauds. Among these, call-centre-based scams have emerged as a major and highly organized threat, often operating across national borders. These scams typically involve fake call centres that impersonate trusted entities such as banks, government agencies, or technical support services to trick individuals into sharing sensitive information or transferring money. This paper examines the structure and functioning of such scam operations in India, highlighting how they have evolved into large-scale, organized networks supported by advanced technologies like VoIP, caller ID spoofing, and cloud-based systems. It also analyses the step-by-step modus operandi of these scams, including victim targeting, psychological manipulation, and money laundering techniques. Further, the study explores the legal framework in India, focusing on the role of the Information Technology Act, 2000 and the Prevention of Money Laundering Act, 2002, along with telecom regulations and enforcement mechanisms. It also discusses the practical challenges faced by authorities, such as cross-border jurisdiction issues, technological anonymity, and gaps in enforcement. Through recent case studies and comparative analysis, the paper demonstrates that call-centre scams are not isolated incidents but part of a broader, organized cybercrime ecosystem. It concludes by emphasizing the need for a coordinated approach involving stronger regulation, improved enforcement, international cooperation, and increased public awareness to effectively tackle this growing threat.

INTRODUCTION

The rapid expansion of digital communication technologies and global connectivity has played a significant role in transforming the nature of crime, giving rise to sophisticated forms of cyber fraud. Among these, call center-based scam operations have emerged as a highly organized and transnational threat. These operations typically involve the establishment of fraudulent call centers that impersonate legitimate institutions such as banks, government authorities, or technical support services, with the objective of deceiving individuals into disclosing sensitive information or transferring money.

In recent years, India has witnessed a noticeable increase in such cyber fraud networks, often operating both domestically and across international borders. These scams are characterized by structured organizational setups, scripted interactions, and psychological manipulation techniques designed to exploit fear, urgency, and trust. The perpetrators frequently employ advanced tools such as Voice over Internet Protocol (VoIP), caller ID spoofing, and data analytics to enhance the

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 5 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

credibility and reach of their fraudulent activities.

1. Nature of Call Center Scam Operation

The call centers in India have moved from being small-scale operations to being industrial-scale operations, leveraging the growth in BPOs, telecommunications infrastructure, and digital payments in the country. They are usually operated by illegal "dark" call centers that pose as legitimate customer service, technical support, or back-office companies, many of which are housed in rented office complexes in cities such as Delhi, Bangalore, Hyderabad, and Vijayawada. Foreign nationals, especially in the US, Japan, and European countries, are the primary targets, although Indian nationals using online banking services and KYC-based services are also increasingly being targeted.

The call centers in India today are not only transnational in their operations but also get their training, infrastructure, and guidance from the larger global fraud networks based in the country. They use VPNs, cloud-based calling platforms, and spoofed caller IDs to make the call appear as if it is originating from a legitimate source such as a bank, the IRS, or companies such as Microsoft, which helps in overcoming the initial skepticism of the victims. Once the victims are "on board" in the minds of the perpetrators, the victims are then intimidated using the fear of being arrested, "digitally arrested," losing their property, facing legal action, etc., in order to force the victims to make rapid money transfers through bank accounts, gift card codes, etc.

According to various academic sources as well as commentary pieces, the call centers in India today have the following organizational structure: "The call centers have HR departments to recruit staff, training programs to teach employees how to 'handle angry targets,' and supervisors who listen in on calls to make sure employees are sticking to the script." The fact that call centers in India today are not only organized but also industrial-scale operations implies that the apprehension of one such call center could lead to the apprehension of hundreds of victims, millions of dollars in losses, as well as a high degree of documentation of the internal operations of the call centers. Hence, the call centers in India today are not only cases of financial crime but also organized cybercrime operations. The problem is especially acute in India because the combination of relatively low infrastructure costs, the availability of a pool of English-speaking youth, as well as the regulatory environment in the country, provides the perfect environment for the growth of call centers in the country.

2. Modus Operandi of Call-Center Scams

Call-center scams operate in several phases: setup, targeting, engagement, closure, and money laundering, all supported by technology and scripted training. Infrastructure and spoofing Scammers rent office space under false legal fronts and install cloud-based SIP calling servers, such as the Eyebeam application. They connect to large volumes of Indian and international phone numbers. By using caller ID spoofing, victims see a phone number that looks like one from a real bank, US government agency, or tech support desk. This tactic increases the chances of the call being answered. These technical tools usually run on live servers that are hard to trace since data doesn't remain on local machines and can be erased quickly during raids. Victim-targeting methods Scammers reach victims through cold calls, fake pop-up alerts in browsers, and phishing emails or texts that urge them to call a "support" number. Some scams target individuals whose personal data has been leaked or bought, allowing agents to know the victim's name, location, or even financial details, which boosts their credibility. In tech support scams, victims may be told that their computer is infected or that their account has a "hacking alert," pressuring them to download remote access software. Psychological manipulation and "digital arrest" Once engaged, scammers follow scripts fine-tuned from previous calls. They may threaten fake "digital arrest," false drug charges, or money laundering allegations,

sometimes displaying forged court warrants or ID cards on screen. In IRS-style or law enforcement impersonation scams, victims are told they need to pay fines or set up "secured accounts" to avoid jail or deportation. These scripts are shared among teams. New recruits learn how to deal with angry or suspicious callers, stay calm under pressure, and repeat standard phrases until the victim agrees to pay. Closure and money extraction "Closer" agents pressure victims to: - Transfer money to "government" or "bank" accounts - Buy gift cards and share the codes - Send funds through wire transfers - Pay into cryptocurrency wallets or online trading platforms controlled by the scammers In some cases, victims install remote access tools, allowing scammers to initiate transfers or access banking apps directly. Layering and laundering Funds move through various mule accounts, prepaid wallets, and cryptocurrency apps, often across different jurisdictions. This makes recovery nearly impossible for victims and tracing difficult for investigators. Some centers even threaten young workers with police complaints, coercing them to participate, which turns the workforce into a mix of willing criminals and vulnerable employees.

Legal Framework in India India's legal response to call-center scams largely relies on the Information Technology Act, 2000 (IT Act), along with the Prevention of Money Laundering Act (PMLA), telecom regulations, and consumer protection measures. The IT Act treats hacking, identity theft, phishing, and impersonation through computer resources as crimes, applicable when scammers fake identities to defraud victims. Sections 66C (identity theft) and 66D (cheating by personation through computer resources) are especially relevant in call-center scams using spoofed caller IDs and fake profiles. The Press Information Bureau (PIB) states that the IT Act empowers authorities to block fraudulent websites and apps involved in these scams. It serves as the foundation of India's cyber law. Additionally, the Enforcement Directorate (ED) uses the PMLA against illegal call-center operators laundering money through various channels. If tax fraud or money laundering is proven, scammers' assets can be seized or frozen. International cooperation helps trace foreign-linked funds. Telecom rules, such as the Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2018), limit unsolicited commercial calls and messages, allowing authorities to penalize or suspend telemarketers who abuse the system. Moreover, the Sanchar Saathi portal (sancharsaathi.gov.in) lets citizens report suspicious numbers, check mobile device security, and request the blocking of SIMs linked to fraud, providing a practical tool for public deterrence. Discussions on consumer law and policy are leaning towards treating fraudulent telemarketing as an unfair trade practice. Proposals suggest adding criminal liability for large-scale or repeat offenders. Together, this mix of cyber law, telecom regulations, anti-money laundering tools, and awareness-building makes up India's evolving legal response to call-center scams, even though enforcement is still inconsistent.

Investigation & Enforcement Challenges Despite several high-profile busts, investigating call-center scams in India faces ongoing challenges. A significant hurdle is the transnational nature of these frauds. Many victims are located in the US, Europe, or Japan, requiring evidence to be collected across jurisdictions, including server logs, financial records, and digital evidence found abroad. This forces Indian agencies to work with foreign law enforcement, such as the FBI, Interpol, and Europol. Different legal standards and data-sharing protocols can delay charges and extradition. Technical obfuscation poses another major issue. Scammers use VPNs, cloud-based calling servers, encrypted apps, and spoofed caller IDs, often leaving no local copies of call records or chats. Even after raids, investigators may only recover partial data. Some centers operate from rented commercial spaces or open-air areas, making continuous surveillance and physical raids challenging. On

the human resource side, centers often hire unemployed youth who view the work as "just a job" and may not fully grasp its criminal nature. This complicates prosecution and deterrence. Some workers face threats of police complaints if they try to leave, further blurring the lines between victim and perpetrator. Regulatory and enforcement gaps remain as well. Although anti-spam and TCCCPR rules exist, enforcement is inconsistent. Many centers temporarily shut down before reopening under new names or in different locations. The proposed stricter treatment of fraudulent telemarketing as a criminal unfair trade practice is still in progress and relies heavily on local police cooperation and public reporting.

Case Studies (Recent Scams) Recent case studies show how call-center scams in India operate on a larger scale with sophisticated methods. CBI busts two illegal call-centers in Delhi (2025) In 2025, the CBI shut down two illegal call centers in Delhi that posed as legitimate customer service operations and defrauded Japanese citizens through tech support scams. Victims were told their electronic devices were compromised and coerced into transferring money to mule accounts. The centers appeared to be genuine customer service hubs. Six individuals were arrested, and multiple assets seized, highlighting Indian agencies' focus on cross-border tech fraud chains. Bengaluru "digital arrest" scam Center (Cybits Solutions, 2025) In 2025, Bengaluru police arrested 16 people running a fake call center under the name Cybits Solutions Pvt Ltd. They targeted US citizens with "digital arrest" and "fake charge" scams. Victims faced threats of fabricated drug-related or money laundering charges and were forced to make digital payments to avoid arrest. Recruits received training in cyber fraud techniques and worked under tight supervision. This case revealed how job listing platforms and interstate recruitment feed into scam centers, making tracking human resources critical. Joint FBI-India probe into $48 million fraud (2026) A joint FBI and Indian investigation shut down three India-based call centers that defrauded over 650 US victims of more than $48 million through tech support and law enforcement impersonation scams. The fraudsters used phone calls, emails, pop-ups, gift cards, bank transfers, and even schemes involving gold bars. Six leaders were arrested in India. This case highlighted how Indian-based centers can create multimillion-dollar global fraud networks, even if most victims never recover their money. ED-led PMLA case against crypto-linked call centers (2026) In early 2026, the Enforcement Directorate (ED) launched a PMLA investigation into large illegal call centers impersonating US government officials. They coerced victims into buying gift cards or making digital payments. The probe linked these centers to cryptocurrency fraud and money laundering, leading to asset freezes and exposing cross-border financial trails. Bengaluru "fake call center" bust (2026) In March 2026, Bengaluru police dismantled a call center using live cloud-based servers for a scam. Workers were trained to impersonate US law enforcement and investigative agency officials. The fraud relied heavily on "digital arrest" threats and fake warrant threats. Some workers were reportedly threatened with police complaints if they tried to leave. These case studies demonstrate that call-center scams in India are not isolated incidents. They are recurring offenses involving organized international victims, layered money flows, and complex digital tactics.

3. Legal Framework in India

India's legal response to call center scams relies mainly on the Information Technology Act, 2000 (IT Act), along with the Prevention of Money Laundering Act (PMLA), telecom regulations, and consumer protection measures. The IT Act classifies offences like hacking, identity theft, phishing, and impersonation over computer resources as criminal acts. These laws can be applied when scammers impersonate banks, government agencies, or companies to defraud victims. Sections 66C (identity theft) and 66D (cheating by impersonation through computer resources)

are especially relevant for call center scams that use fake caller IDs and profiles. The Press Information Bureau (PIB) states that the IT Act allows authorities to block fraudulent websites and apps used in these scams. It serves as the foundation of India's cyber law framework. Additionally, the Enforcement Directorate (ED) uses the PMLA against illegal call center operators who launder money using bank accounts, wallets, and crypto channels. If links to tax fraud or money laundering are established, officials can seize or freeze the assets of the scam operators, and they can trace foreign funds through international cooperation. Telecom rules, like the Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2018), limit unsolicited commercial calls and SMS. They also allow authorities to penalize or suspend telemarketers who misuse the system. The Sanchar Saathi portal (sancharsaathi.gov.in) lets citizens report suspicious numbers, check mobile device security, and request blocking of SIMs.

4. Investigation and Enforcement Challenges

Despite repeated high-profile busts, investigating call-center scams in India faces several ongoing challenges. A major hurdle is the international nature of these frauds. Many victims are in the US, Europe, or Japan, so evidence must be collected from different jurisdictions. This includes server logs, financial records, and digital evidence located abroad. Indian agencies must coordinate with foreign law enforcement, such as the FBI, Interpol, and Europol. This coordination can delay charges and extradition due to varying legal standards and data-sharing protocols.

Technical obfuscation is another significant problem. Fraudsters use VPNs, cloud-based calling servers, encrypted apps, and fake caller IDs. They often do not store local copies of call records or chats, so even when raids happen, investigators may only recover partial data. Some centers operate from rented commercial buildings or even open-air spaces that allow for quick escapes. This makes continuous surveillance and physical raids difficult.

On the human-resource side, centers often hire unemployed youth who view such work as "just a job." Many are not fully aware of the illegal nature of what they are doing. This complicates prosecution and deterrence. Some workers are even threatened with police complaints if they quit, further blurring the line between victim and perpetrator.

Regulatory and enforcement gaps also exist. While anti-spam and TCCCPR rules are in place, enforcement is inconsistent. Many centers simply shut down temporarily and reopen under new names or locations. The proposed tougher measures against fraudulent telemarketing as a criminal-level unfair trade practice are still being implemented. These measures rely heavily on local police cooperation and public reporting rates.

5. Case Studies (recent scams)

Recent cases clearly show that call-centre scams in India are being carried out on a large scale, with well-planned and increasingly sophisticated methods.

- CBI busts two illegal call centres in Delhi (2025)

In 2025, the CBI shut down two illegal call centres in Delhi that were pretending to be genuine customer service operations. They targeted Japanese citizens through tech-support scams, convincing victims that their devices had been hacked or compromised. The callers pressured them into transferring money to fake accounts. These centres were carefully set up to look like legitimate offices. Six people were arrested, and several assets were seized. This case highlights how Indian authorities are now actively focusing on international cyber fraud networks.

- Bengaluru "digital arrest" scam centre (Cybits Solutions, 2025)

In the same year, Bengaluru police arrested 16 individuals running a fake call centre under the name Cybits Solutions Pvt Ltd. They targeted people in the United States using "digital arrest" scams, where victims were threatened with fake

charges like drug trafficking or money laundering. Out of fear, victims were forced to make digital payments to avoid supposed arrest. Employees working there were trained in fraud techniques and closely monitored. This case also showed how scammers use job portals and recruit people from different states, making tracking of human resources more important.

- Joint FBI–India probe into $48 million fraud (2026)

In 2026, a joint investigation by the FBI and Indian authorities led to the shutdown of three call centres in India. These centres had scammed over 650 victims in the US, stealing more than $48 million. They used various methods like phone calls, emails, pop-ups, and even schemes involving gift cards, bank transfers, and gold bars. Six main accused were arrested in India. The case shows how these operations can run globally and generate huge amounts of illegal money, while victims often struggle to recover their losses.

- ED investigation under PMLA into crypto-linked scams (2026)

In early 2026, the Enforcement Directorate began investigating illegal call centres under the Prevention of Money Laundering Act (PMLA). These centres impersonated US government officials and pressured victims into making payments through gift cards or digital methods. The investigation revealed links to cryptocurrency fraud and money laundering. Authorities froze assets and traced financial transactions across borders.

- Bengaluru fake call centre bust (2026)

In March 2026, Bengaluru police uncovered another scam operation that used cloud-based servers to run fake call-centre activities. Workers were trained to impersonate US law enforcement officials and scare victims using fake warrants and "digital arrest" threats. In some cases, employees themselves were threatened with legal action if they tried to leave the job.

6. Comparative Analysis

You can compare India's call-centre scam ecosystem with other countries (e.g., Philippines, Colombia, Nigeria) along axes such as targeting profile, legal-regime strength, and enforcement outcomes.

Aspect	India (call-centre scams)	Example: Philippines / Colombia (scam-centres)
Core scam types	Tech-support, bank-fraud, "digital arrest," IRS-style impersonation	Tax-fraud, lottery, romance-scam, and small-ticket phishing-style calls
Victim geography	Mostly foreign nationals (US, Japan, Europe) and overseas Indians	Mix of local and global victims, often via social-media-linked scams
Legal backbone	IT Act 2000, PMLA, TRAI-related telecom rules, and Sanchar Saathi	Cyber-crime laws plus telecom-fraud regulations, often with stronger extradition frameworks in some cases
Enforcement model	CBI, state cyber-crime cells, ED, DoT, and joint-investigations with FBI/Interpol	Dedicated cyber-crime units plus international-cooperation agencies, with faster case-closure in some regions

This comparative table highlights how India shares core traits with other scam-hub countries such as impersonation-based fraud and layered money-laundering but also faces

unique challenges in integrating telecom-regulation, corporate-BPO oversight, and cross-border enforcement.

7. Relevant Laws from Information Technology Act, 2000

Section 43 – Penalty and compensation for damage to computer system, etc.

If any person, without permission of the owner or person in charge of a computer, computer system or network— (a) accesses or secures access;
(b) downloads, copies or extracts any data or information;
(c) introduces any computer contaminant or virus;
(d) damages or disrupts any system;
(e) denies access to any authorized user;
(f) provides assistance to facilitate unauthorized access;
(g) charges services to another person's account;
he shall be liable to pay damages by way of compensation.

Section 65 – Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys, or alters any computer source code required to be kept by law shall be punishable with imprisonment up to three years, or with fine up to two lakh rupees, or with both.

Section 66 – Computer-related offences

If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment up to three years or with fine up to five lakh rupees, or with both.

Section 66B – Dishonestly receiving stolen computer resource

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing it to be stolen shall be punished with imprisonment up to three years or with fine up to one lakh rupees, or with both.

Section 66C – Identity theft

Whoever fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of another person shall be punished with imprisonment up to three years and fine up to one lakh rupees.

Section 66D – Cheating by personation using computer resources

Whoever, by means of any communication device or computer resource, cheats by personation shall be punished with imprisonment up to three years and fine up to one lakh rupees.

Section 66E – Violation of privacy

Whoever intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without consent shall be punished with imprisonment up to three years or with fine up to two lakh rupees, or with both.

Section 66F – Cyber terrorism

Whoever, with intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror, denies access to a computer resource, attempts unauthorized access, or introduces contaminants causing or likely to cause death, injuries, or disruption of essential services, shall be punishable with imprisonment for life.

Section 67 – Publishing obscene content in electronic form

Whoever publishes or transmits or causes to be published in electronic form any material which is obscene shall be punished on first conviction with imprisonment up to three years and fine up to five lakh rupees, and on subsequent conviction with imprisonment up to five years and fine up to ten lakh rupees.

CONCLUSION

To effectively deal with call-centre scams, India needs a practical and multi-layered approach. This includes stricter licensing and regular monitoring of BPOs and call centres, along with better systems to quickly identify and block fraudulent phone numbers. Telecom operators and digital platforms should also be held more accountable when their services are misused for spoofed calls or unsafe communication. At the same time, authorities must strengthen international cooperation by speeding up evidence-sharing with agencies like the Federal Bureau of Investigation and Europol. Investment

in advanced digital forensics is equally important to track cloud-based servers and cryptocurrency transactions. Public awareness also plays a key role—campaigns through banks, social media, and initiatives like Sanchar Saathi should consistently remind people not to share OTPs, card details, or allow remote access to unknown callers.

Call-centre scams in India have evolved beyond small-scale fraud into highly organized, large-scale cybercrime operations. These networks take advantage of India's strengths in language skills, telecom infrastructure, and service sectors. Unless there is a balanced approach that combines stricter laws, more effective enforcement, and widespread public awareness, such scams will continue to siphon huge amounts of money from victims across the world, ultimately affecting trust in India's growing digital economy.

REFERENCES

1. 'CBI Busts 2 Illegal Call Centres in Delhi, 6 Scammers Arrested' *Hindustan Times* (29 May 2025) https://www.hindustantimes.com/india-news/cbi-busts-2-illegal-call-centers-in-delhi-6-scammers-arrested-101748504857672.html
2. 'Multimillion-dollar Fraud Probe in Maryland Leads to Call Centers in India' *The Daily Record* (3 February 2026) https://thedailyrecord.com/2026/02/03/fbi-india-call-center-scam-investigation/
3. 'Fake Call Centre in Bengaluru Busted for Digital Arrest Scam, 16 Arrested' *NDTV* (14 October 2025) https://www.ndtv.com/bangalore-news/fake-call-centre-in-bengaluru-busted-for-digital-arrest-scam-16-arrested-9452251
4. 'How Indian Scammers Built a Multi-Billion-Dollar Global Fraud Empire' *TRT World* (3 June 2025) https://www.trtworld.com/article/23e1fe1c3220
5. 'Fake Call Centre Scam Busted' *Bangalore Mirror* (7 October 2025) https://bangaloremirror.indiatimes.com/bangalore/crime/fake-call-centre-scam-busted/articleshow/126164080.cms
6. 'Press Note Details' *Press Information Bureau, Government of India* https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3&reg=3&lang=2
7. 'ED Busts Illegal Call Centre, Operators Posed as US Govt Officials' *Deccan Herald* (10 February 2026) https://www.deccanherald.com/india/ed-busts-illegal-call-centre-operators-posed-as-us-govt-officials-3893525
8. 'Soon-to-be Unfair Trade Practice: Telemarketing, Fraudulent Calls to Incur Criminal Liability' *The Economic Times* (13 May 2024) https://economictimes.indiatimes.com/industry/telecom/telecom-news/soon-to-be-unfair-trade-practice-telemarketing-fraudulent-calls-to-incur-criminal-liability/printarticle/110094275.cms