

# Indian Call Center Scam Checklist (PDF): 50+ Red Flags to Spot a Fraud Call

Scammers operating from call centers, often based in India, use high-pressure tactics to trick victims into handing over money or personal information. Whether it's a fake **tech support call**, **IRS scam**, or **banking fraud**, these scammers follow predictable patterns. Use this **detailed checklist** to **identify red flags**, **protect yourself**, and avoid falling victim to fraudulent calls. **The more red flags you check, the higher the risk—stay alert!** 🚩

---

## Indian Call Center Scam Detection Checklist

 The more boxes you check, the more likely it's a scam.

---

### 1 Call Origin & Identity Check

- ☐ Caller ID shows an unknown or international number (often from India, Pakistan, Philippines, etc.)
  - ☐ Caller uses a generic, Western-sounding fake name (e.g., "John Smith" or "David Johnson")
  - ☐ Call comes from a "spoofed" number (appears local but is actually international)
  - ☐ Caller avoids giving a **direct company name** or says something vague like "Technical Support"
  - ☐ Number is unlisted or cannot be found online in connection with a legitimate company
- 

### 2 Call Script & Pressure Tactics

- ☐ Caller is reading from a script, repeating phrases in a robotic or unnatural way

- ☐ Caller speaks with a thick accent but claims to be from an American/European company
  - ☐ Urgency is emphasized—caller insists you must **act immediately** or face dire consequences
  - ☐ You are told you owe **taxes, fines, or payments** and must pay immediately to avoid legal action
  - ☐ Threats are made: jail time, lawsuits, arrest, or suspension of services
  - ☐ Caller refuses to let you hang up, **keeping you on the line as long as possible**
  - ☐ Caller uses scare tactics, claiming your device is infected, your bank account is in danger, or your identity has been stolen
- 

### **Common Scam Types & Signs**

#### **Tech Support Scam**

- ☐ You get an unsolicited call about viruses, malware, or issues with your computer
- ☐ Caller claims to be from **Microsoft, Apple, Dell, or Amazon Tech Support**
- ☐ You are asked to download **remote access software** (e.g., AnyDesk, TeamViewer, UltraViewer)
- ☐ Caller asks for **credit card details or payment** for a fake service
- ☐ A fake refund is "accidentally" given, and they demand the excess be returned

#### **IRS/Tax Fraud Scam**

- ☐ Caller claims to be from the **IRS, CRA, or other tax authorities**
- ☐ They demand immediate payment for a tax debt
- ☐ You are told to pay via **gift cards, cryptocurrency, or wire transfer**
- ☐ You are threatened with **deportation, lawsuits, or arrest**

#### **Banking & Financial Scam**

- ☐ Caller claims to be from **your bank, PayPal, or another financial institution**
- ☐ They ask for **account details, PINs, or online banking login information**

- ☐ You receive a **fraud alert** call but are asked to verify details by providing security codes

### ◆ **Government or Immigration Scam**

- ☐ Caller pretends to be from **U.S. Immigration, Social Security, or another government agency**
- ☐ They say your **passport, visa, or Social Security number is at risk**
- ☐ You are pressured into making a **fine payment immediately**

### ◆ **Loan & Grant Scam**

- ☐ Caller offers a **pre-approved loan or grant** but requires upfront payment
- ☐ You must pay a **"processing fee" or "verification fee"** to receive the funds

### ◆ **Lottery & Prize Scam**

- ☐ You are told you won a lottery, sweepstakes, or grand prize **you never entered**
- ☐ They require **payment or personal details** to "claim" your winnings

### ◆ **Job & Work-From-Home Scam**

- ☐ You receive an unsolicited job offer with **high pay and no experience required**
- ☐ A fee is required upfront for **training materials or equipment**
- ☐ You are asked to **cash a check and send part of the money back**

---

## **4 Payment & Financial Red Flags**

- ☐ You are asked to pay via **gift cards (Google Play, Amazon, iTunes, etc.)**
  - ☐ Payment is requested through **cryptocurrency (Bitcoin, Ethereum, etc.)**
  - ☐ Caller asks you to send money via **Western Union, MoneyGram, or an untraceable wire transfer**
  - ☐ They refuse to accept payment via **credit card or regular banking methods**
  - ☐ Caller tries to convince you that **a legitimate business practice is unusual** (e.g., "Banks don't allow refunds, so we need to use gift cards")
-

## 5 Online & Remote Access Requests

- ☐ Caller asks you to **download software for remote access**
  - ☐ You are directed to a **strange website or a link via email**
  - ☐ You are told to install an app **outside of official stores (Google Play, Apple Store)**
  - ☐ Caller requests **screen sharing** to “help solve a problem”
- 





## 6 Language & Behavioral Red Flags

- ☐ Caller speaks in a **thick accent** but claims to be from an American/European organization
  - ☐ Call quality is poor—echoes, background noise of a large call center
  - ☐ Caller gets **angry, aggressive, or frustrated** if you ask too many questions
  - ☐ When challenged, they **hang up suddenly** or pass you to another fake “supervisor”
- 

## 7 Verification & Fact-Checking Steps

- ☐ **Google the phone number**—if it’s a known scam, it will likely appear in scam reports
  - ☐ **Look up the official company number** and call back yourself
  - ☐ **Ask for their employee ID**—most scammers will make up fake credentials
  - ☐ **Never share personal details** unless you initiated the contact
  - ☐ **Check government and scam reporting sites** (FTC, BBB, IRS, etc.) for warnings
- 

## Final Assessment: Is It a Scam?

-  **0-5 Flags:** Low risk—may still be worth investigating
  -  **6-10 Flags:** Medium risk—be cautious, verify details
  -  **11-15 Flags:** High risk—very likely a scam, do not engage
  -  **16+ Flags: 100% SCAM**—hang up immediately and report it!
-

## ✅ What to Do If You Detect a Scam:

1. **Hang up immediately**—do not engage
  2. **Do NOT share personal, financial, or banking details**
  3. **Block the number** and report it to scam monitoring websites
  4. **If you've sent money, contact your bank or card provider ASAP**
  5. **Report the scam to local authorities (FTC, IRS, Interpol, or cybercrime units)**
- 

## 🚨 Stay Safe & Informed! 🚨

Indian call center scams **evolve constantly**, so always stay skeptical of **unverified calls** asking for money or personal data. If in doubt, **hang up and verify independently**.

## About This Document

© Faisal Khan LLC. This document is designed as a resource for professionals and entrepreneurs in the banking, payments, and financial services sectors. It aims to guide strategic planning and decision-making for businesses exploring innovative financial solutions. For more comprehensive resources and expert insights:

- Visit our website: <https://faisalkhan.com>
- Explore our Banking and Payments Wiki: <https://faisalkhan.com/knowledge-center/payments-wiki/>

© Faisal Khan LLC. All rights reserved. This document may be shared or redistributed for non-commercial purposes with proper attribution to Faisal Khan LLC. Unauthorized commercial use, reproduction, or distribution without prior written consent is prohibited.

---

### Faisal Khan LLC

Cross-Border Payments & Financial Consulting Experts

Website: [www.faisalkhan.com](http://www.faisalkhan.com) | Email: [Contact Us Page](#)

*"Your trusted partner in banking, payments, and licensing solutions."*

