

Federal Advisory Warns of Rising Cross-Border Call Center Scams Targeting US Citizens

D.C, WA, UNITED STATES, September 28, 2026 /EINPresswire.com/ -- Sophisticated Indian cyber scam networks based in India have grown into a massive, multibillion-dollar illegal business. Over just three years, these operations stole more than \$1 billion from U.S. citizens using tech support and government impersonation scams. Globally, these scattered criminal networks cause about \$10 billion in losses every year, according to research from the Indian Institute of Technology Kanpur.



The rapid shift of call center fraud from small operations in rural villages to highly organized corporate setups has forced the Federal Trade Commission (FTC) and the Federal Bureau of Investigation (FBI) to step up their enforcement. This rise shows how international crime is changing. Digital tools now allow criminals to target vulnerable people from thousands of miles away. Over time, these operations have grown from amateur phone scams into professional businesses that use clever social engineering tricks to fool people.

From Village Operations to Corporate Syndicates

Investigators have traced the main hubs of this activity to the Jamtara district in Jharkhand and the Mewat region, which spans parts of Haryana and Rajasthan. Once known for local crime, entire villages in these areas now run like organized, decentralized call centers. Tech administrators use Voice over Internet Protocol (VoIP) servers, virtual private networks (VPNs), and spoofing software to hide where the calls are really coming from, making international calls look like local U.S. area codes.

Financially, these hubs operate just like modern corporate call centers. "They have dedicated scriptwriters, quality compliance managers, and complex money-laundering systems that use digital currency, wire transfers, and gift card mules," said Michael Harrison, a senior

cybersecurity analyst.

The Four Main Ways These Scams Work

Federal authorities group the main methods used by these international networks into four categories:

- Tech Support Scams: Victims see aggressive pop-up messages on their computers warning about system failures, malware, or security breaches. Scammers pretending to be certified tech support engineers take remote control of the computer to charge fees for useless software fixes or security subscriptions.
- Government Impersonation: Scammers claim to be from major federal agencies like the Internal Revenue Service (IRS) or the Social Security Administration (SSA). They threaten victims with immediate arrest, lawsuits, or losing their property over fake tax or legal debts.
- Digital Arrests: A growing twist on government scams forces victims to stay on continuous, encrypted video calls. Scammers wearing fake law enforcement uniforms with realistic court backdrops scare people into transferring their money to fake verification accounts.
- Refund Fraud: Fake e-commerce emails or texts trick victims into calling a fake customer service line. The scammers then claim they accidentally refunded too much money and pressure the victim into returning the difference through cryptocurrency kiosks or wire transfers.

Institutional Challenges and Enforcement Gaps

According to data from the FBI's Internet Crime Complaint Center (IC3), tech support scams alone brought in more than 40,000 complaints and cost Americans over \$1 billion in a single year.

Stopping these international networks is incredibly difficult for Western law enforcement due to legal boundaries and distance. While the FBI's IC3 shares data quickly, executing physical raids and extraditing suspects requires long diplomatic and bureaucratic teamwork with Indian authorities.

"Fraudsters don't work within borders, they don't work on jurisdictions; they work on opportunities," an FBI official said in a recent Department of Justice enforcement briefing. "And so we need to be able to have that data across all of our agencies in order to identify trends and more strategically pursue large, enterprise investigations."

On top of that, scammers move stolen money incredibly fast, making it hard to recover. The stolen cash is quickly funneled through decentralized finance networks or turned into untraceable gift cards, leaving the financial system in minutes. Older Americans remain the biggest target. IC3 reports show that people over 60 suffer the highest financial losses, often because they are less familiar with digital tech and more likely to trust authority figures.

How to Protect Yourself and Report Scams

Federal consumer protection officials say that public education and double-checking facts are the best ways to fight back. An official FTC scam warning lists key rules to stay safe:

- Verify Independently: Government agencies will never threaten to arrest you over the phone, demand immediate payment in cryptocurrency, or ask for gift card numbers.
- Deny Remote Access: Never let someone who called you out of the blue or a random internet pop-up take control of your computer screen.
- Hang Up: End suspicious calls immediately. Look up the organization's official public contact info yourself instead of calling numbers from unexpected messages.

If you have been targeted by an India-based cyber scam or see a scam attempt, you should report it right away. Filing a complaint through the official FBI IC3 Portal helps investigators track digital footprints and spot broader trends. You can also log any suspected scams through the FTC Fraud Reporting Portal to help consumer protection lawyers track new tricks and take down the digital infrastructure scammers rely on.

For a deeper look into how these international networks operate, you can read the full investigative report published on [The Diplomat](#).

Additional coverage is available on [WeNews English](#).

Michael Carter
Global Scam Awareness Network
NumaPapi@proton.me

This press release can be viewed online at: <https://www.einpresswire.com/article/945788939>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.