The New Cybercrime Hub: Beyond National Identity

Reported scam investigations in India highlight the need for evidence-based scrutiny, stronger oversight, and international cooperation.

The New Cybercrime Hub by Akmal Joned

NEW YORK CITY, NY, UNITED STATES, October 26, 2026 /EINPresswire.com/ -- Cybercrime is increasingly intertwined with national identity and geopolitical rivalry. Yet the growing international attention surrounding cybercriminal networks should not obscure another important development: India is also emerging as a significant location in the global landscape of online fraud.

On September 17, 2026, The Indian Express reported that India's Enforcement Directorate (ED), which investigates financial crimes and money laundering, had raided three call centres in Pune and Patiala. Approximately 220 people were reportedly found working at the locations. Investigators alleged that the centres were involved in defrauding and extorting American citizens through deceptive payment claims. Authorities were also tracing individuals suspected of coordinating the operations and managing their proceeds.

The case raises important questions about India's expanding role in cross-border online fraud. Although a single investigation cannot establish that India is the world's largest scam hub, it demonstrates why the country deserves closer international scrutiny. The challenge is to determine whether such operations represent isolated criminal enterprises or part of a broader pattern of organised digital fraud.

India and the Expanding Geography of Online Scams

Online scams are no longer simply the work of isolated individuals operating from private computers. Increasingly, they involve organised networks that combine digital communications, psychological manipulation, coordinated labour, and sophisticated financial transactions. Call

centres can provide an operational structure through which perpetrators impersonate officials, misrepresent financial obligations, and pressure victims into transferring money.

India's extensive telecommunications infrastructure, large workforce, and established business-services sector provide legitimate economic advantages. However, these same capabilities can also be exploited by criminal networks. Fraudulent operations may disguise themselves as legitimate commercial enterprises, making it difficult to distinguish lawful businesses from organised criminal activity without effective oversight and investigation.

A report published by The Diplomat in October 2026 also examined scam operations in India, including alleged schemes targeting American citizens. Together, these reports reinforce the need to examine India's role in international online fraud more closely.

The central concern is not India's national identity, but whether criminal organisations are exploiting its infrastructure, workforce, and financial systems to reach victims abroad. Nevertheless, a distinction must be maintained between documented criminal cases and claims about the overall scale of the problem. Establishing whether India is a leading global centre for online scams would require comprehensive comparative data on the number of operations, financial losses, victim locations, and the geographical origins of criminal networks. Such evidence should inform the debate rather than assumptions or political rhetoric.

American Victims of Scams Based in India

The alleged targeting of American citizens is particularly significant. It highlights the reach of cross-border fraud. Even societies with advanced digital infrastructure, sophisticated banking systems, and substantial law-enforcement resources remain vulnerable to transnational criminal networks.

In September 2025, the US Department of the Treasury reported that Americans had lost more than US$10 billion to scams originating in Southeast Asia during 2024. This figure concerns Southeast Asia and should not be attributed to India. It provides regional context rather than a measure of the losses linked to the Indian cases. Nevertheless, it illustrates the scale of the wider regional threat and the importance of identifying the specific locations and networks responsible.

Against this broader backdrop, the reported cases in India raise questions about the effectiveness of regulatory supervision, financial monitoring, and law-enforcement coordination. If fraudulent call centres can operate under the appearance of legitimate businesses while targeting victims overseas, authorities must examine whether existing safeguards are adequate. Repeated discoveries of such operations would strengthen the case for more rigorous oversight and enforcement.

Beyond domestic enforcement, the international response to cybercrime must avoid selective

scrutiny. Strategic partnerships, economic interests, and diplomatic considerations should never determine whether credible allegations receive proper attention. At the same time, the presence of criminal networks within a country's territory does not automatically establish government involvement or complicity. Allegations of official protection must be supported by independent evidence. Accountability should focus on the organisers, financial facilitators, and other individuals proven to have enabled these activities, rather than the entire population of the country.

In this context, India's emerging significance in discussions about online scams should be approached as a serious law-enforcement and governance concern, not as an argument against Indian society as a whole. The critical question is whether the authorities can effectively identify criminal operations, dismantle their networks, recover illicit proceeds, and prevent their recurrence.

Effective action requires more than occasional raids. Investigators must trace financial transactions, identify the controllers behind fraudulent call centres, strengthen cooperation with foreign law-enforcement agencies, and pursue criminal proceeds across jurisdictions. Authorities must also distinguish between willing participants and individuals who may have been coerced, deceived, or trafficked into working at scam facilities.

Ultimately, India's position in the global digital economy brings both opportunities and responsibilities. Its technological capacity and workforce can support legitimate international business, but these advantages must not become cover for organised fraud. If evidence increasingly identifies India as a major operational base for online scams, that finding deserves sustained international attention and a stronger domestic response.

The objective is not to replace one national scapegoat with another. It is to recognise that online fraud has become a transnational industry capable of exploiting national infrastructure, regulatory weaknesses, and gaps in international cooperation. India's growing presence in reported scam investigations makes it an important part of this debate. The credibility of the response will depend on transparency, consistent enforcement, and the willingness to confront criminal activity wherever the evidence leads.

The main challenge is not to identify a nation to blame, but to ensure that criminal networks cannot hide behind national borders or exploit rivalries among major powers. Cybercrime has no nationality.

For review copies, interview requests, or additional information, please contact:

Akmal Joned
BrightKey PR
media@brightkeypr.com

This press release can be viewed online at: https://www.einpresswire.com/article/952416296

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.