Federal Communications Commission

Improving Customer Service and Protecting Consumers Through Onshoring

47 CFR Parts 8, 25, 64 and 76
[CG Docket Nos. 26-52, 17-59, 02-278, and 22-2; FCC 26-16; FR ID 341337]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Washington, DC
May 26, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Scammers, some of whom maintain tacit ties to foreign adversaries, are increasingly targeting American consumers as a lucrative source of income. According to the FBI, Chinese-linked scam operators have collectively stolen billions from unsuspecting victims, many of whom are senior citizens, placing strain on tens of thousands of families across the country. According to the Department of Homeland Security, fraudulent messages tied to purported overdue highway tolls and payments for packages alone generated $1 billion from 2022 to 2025.[1]

In addition to relying on sophisticated spoofing techniques, these scams leverage call centers overseas as cover for illicit activity. While operating apart from legitimate businesses, scammers can exploit these firms as sources for labor and cellular infrastructure, while also laundering fraudulent funds through these businesses. Once embedded within a local economy, these operations can proliferate as criminal networks share tactics, commercialize scamming techniques at scale, and fund regional instability.

The Federal Communications Commission (FCC) can combat this proliferation by strengthening protection for consumer information while raising awareness among the American public. Though not a law enforcement organization that can prosecute scammers, the commission can raise barriers to entry for foreign scammers operating on U.S. networks, rigorously enforce stronger data security protections, and inform consumers of the risks involved in sharing certain types of sensitive information.

Scammers Maintain Ties to Adversarial Governments

Though often viewed through the lens of law enforcement, these scams present a national security threat. Chinese criminal organizations, often with the complicity of Beijing, have established large-scale operations across Southeast Asia to exploit lax law enforcement and press locals into forced labor.[2] They are also key drivers of regional instability, including among U.S. allies and partners. During a brief border clash between Thailand and Cambodia in 2025, Thai armed forces targeted hotels and compounds housing scam centers amid its "war on the Scam Army" while scam compounds in Myanmar funnel funds to armed rebel groups seeking to combat the ruling military junta.[3]

Meanwhile, North Korean scammers, many of whom receive significant support from Chinese counterparts, collectively generate billions for the regime's weapons program. This issue has

[1] Robert McMillan, "Chinese Criminals Made More Than $1 Billion From Those Annoying Texts," *The Wall Street Journal*, October 14, 2025. (https://www.wsj.com/tech/cybersecurity/url-scam-texts-china-gangs-68e96097)
[2] Nathan Picarsic, "Made in China, Paid by Seniors: Stopping the Surge of International Scams," *Testimony before the Senate Special Committee on Aging*, January 14, 2026. (https://www.fdd.org/analysis/2026/01/14/made-in-china-paid-by-seniors-stopping-the-surge-of-international-scams)
[3] Sui-Lee Wee, "Thailand, Attacking Cambodia, Says Its Target Is the Scam Industry," *The New York Times*, December 24, 2025. (https://www.nytimes.com/2025/12/24/world/asia/cambodia-scam-centers-refugees-thailand.html)

caught the attention of the FBI, which has previously warned of North Korean scammers using Chinese operations and tactics to target Western firms, particularly offshored IT support.[4]

Legitimate Foreign Call Centers Can Provide Cover to Illicit Scam Operations

While most foreign call centers servicing the American market are legitimate businesses, their presence in certain markets, particularly across Southeast Asia, can offer effective cover to illicit scamming operations that steal billions from American consumers.

Fraudulent scam centers across Southeast Asia often rely on the presence of legitimate call centers to trap migrants and impoverished local residents by falsely advertising open positions at those centers across social media and on local job posting boards. These scams are often elaborate, including spoofed email addresses from mainstream companies, multi-stage interview processes, and arranged travel to rural locations, to lure in jobseekers looking for Western-facing business opportunities.[5] INTERPOL has previously documented that these false opportunities have trapped hundreds of thousands of human trafficking victims across the region, many of whom are forced to work imprisoned within scam compounds, where they are often beaten and sexually assaulted by superiors.[6]

These scams also operate on cross-border telecoms infrastructure used by legitimate call centers. As part of cracking down on persistent cyber-enabled scam operations, Thailand began cutting international private telecommunications links to a series of Cambodian operators due to their alleged criminal behavior, highlighting the role of an integrated telecoms supply chain in tying together illicit and legitimate operators.[7] Illicit operators also often rely on tools such as "SIM boxes" that may contain dozens of SIM cards to target victims using legitimate carrier infrastructure.[8]

The operation of both scam and legitimate call centers also raises the prospect of the former using the latter as a vehicle for money laundering. This issue is particularly persistent within

---

[4] U.S. Department of Justice, Press Release, "Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea," January 23, 2025. (https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote)

[5] Hai Thanh Luong, "'Simple job, high salary': unveiling the complexity of scam-forced criminality in Southeast Asia," *Nature*, August 12, 2025. (https://www.nature.com/articles/s41599-025-05605-1); Randall Hansen, "Inside Southeast Asia's scam compounds: A trafficked worker tells of fraud, coercion and torture," *The Conversation*, April 15, 2026. (https://theconversation.com/inside-southeast-asias-scam-compounds-a-trafficked-worker-tells-of-fraud-coercion-and-torture-280311)

[6] INTERPOL, "Growing threat of transnational scam centres highlighted at INTERPOL General Assembly," November 26, 2025. (https://www.interpol.int/en/News-and-Events/News/2025/Growing-threat-of-transnational-scam-centres-highlighted-at-INTERPOL-General-Assembly); INTERPOL, "INTERPOL releases new information on globalization of scam centres," June 30, 2025. (https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres)

[7] "Thailand cuts all internet links to Cambodia," *Bangkok Post* (Thailand), June 26, 2025. (https://www.bangkokpost.com/thailand/general/3058685/thailand-cuts-all-internet-links-to-cambodia)

[8] "Illegal Robocalls and Call-Based Fraud," *US Telecom*, July 31, 2025. (https://ustelecom.org/illegal-robocalls-and-call-based-fraud)

Southeast Asia, as scam centers often operate with the tacit endorsement of local political authorities.[9] Scam centers flourish under the cover of both legitimate commercial operations and restrained legal scrutiny. Scam centers also often use legitimate licenses for business process offshoring to cover their illicit trafficking and phone-based fraud. Lucky South 99 in the Philippines, for example, originally received a legitimate license to act as a business process outsourcing hub, even as the firm operated as one of the country's largest scam centers until it was raided by Filipino authorities in June 2024.[10]

Technology Is Amplifying the Threat

Relying on commercial technology, scammers have scaled their operations with relatively little investment. Relying on voice over internet protocol (VoIP) providers, scam operations often spoof well-known companies or local area codes to trick victims into providing personal financial information or other assets such as cryptocurrencies or gift cards.[11] Scammers can run dozens of spoofed numbers in parallel from a single central "SIM farm," sending millions of messages using relatively limited set-ups.[12] The rise in VoIP has also allowed scammers to integrate more cyber tools into their efforts, including using artificial intelligence (AI) to automate portions of the attacks before funneling responsive victims to a human operator to facilitate further theft and using AI for more sophisticated social engineering attacks such as mimicking known voices.[13]

These technologies are not bespoke; they are increasingly off-the-shelf packages that can easily be sold and proliferate. Scamming operations have turned toward the open market to sell their technology to other criminal actors, either for a quick profit or for a portion of extorted funds. These sales often launch subsequent waves of similar attacks against U.S. consumers — new Chinese kits for SMS phishing led to a significant rise in false messages ostensibly from state toll agencies flooding both Apple and Android devices over the past year.[14]

---

[9] U.S.-China Economic and Security Review Commission, "China's Exploitation of Scam Centers in Southeast Asia," July 18, 2025. (https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia); Nathan Picarsic, "Made in China, Paid by Seniors: Stopping the Surge of International Scams," *Testimony before the Senate Special Committee on Aging*, January 14, 2026. (https://www.fdd.org/analysis/2026/01/14/made-in-china-paid-by-seniors-stopping-the-surge-of-international-scams)

[10] Richmond Mercurio, "SEC revokes Lucky South 99 registration," *The Philippine Star* (The Philippines), August 29, 2024. (https://www.philstar.com/headlines/2024/08/29/2381331/sec-revokes-lucky-south-99-registration); Department of Justice of the Philippines, "Amid Illegal POGO Issues, Remulla Warns Erring Aliens of 'Extreme' Legal Repercussions," June 9, 2024. (https://www.doj.gov.ph/news_article.html?newsid=H8XR9vxNB4BDut89WxJbURsadw6wVl0Am8mBHYulMes)

[11] "Illegal Robocalls and Call-Based Fraud," *US Telecom*, July 31, 2025. (https://ustelecom.org/illegal-robocalls-and-call-based-fraud); Keven Hendricks, "Investigating Scam Phone Calls," *Federal Bureau of Investigation*, June 10, 2020. (https://leb.fbi.gov/articles/featured-articles/investigating-scam-phone-calls)

[12] Kevin Ozebek, "Millions of scam texts being generated in LA, security expert says," *ABC7*, November 10, 2025. (https://abc7.com/post/millions-scam-texts-being-generated-la-sim-farms-security-expert-says/18126320)

[13] "How vishing and AI voice cloning attacks target businesses," *Threat Locker*, March 27, 2026. (https://www.threatlocker.com/blog/ai-voice-cloning-and-vishing-attacks-what-every-business-must-know); Mike Winters, "AI-powered scam calls are getting more convincing—and more common: 'It was her voice, I know her scared cry,'" *CNBC*, May 9, 2026. (https://www.cnbc.com/2026/05/09/ai-powered-scam-calls-getting-more-convincing.html)

[14] Brian Krebs, "Chinese Innovations Spawn Wave of Toll Phishing Via SMS," *KrebsonSecurity*, January 16, 2025. (https://krebsonsecurity.com/2025/01/chinese-innovations-spawn-wave-of-toll-phishing-via-sms); Robert McMillan,

Recommendations

While the FCC cannot fully prevent foreign scammers from relying on legitimate offshore call centers to target American customers, the commission can provide consumers with greater information to potentially modify their behavior when interacting over the phone. In doing so, the commission's goal should be to protect Americans by forcing providers of telecommunications services, CMRS, interconnected VoIP service, cable television service, and DBS services, or affiliates of such providers, to proactively secure their operations while providing avenues for administrative recourse.

- **The FCC should require all providers to inform customers of their use of a foreign call center each time a call is handled outside of the United States**. The FCC should ensure that providers offer clarity to consumers, potentially allowing them to either modify their behavior in sharing certain information or simply recognize the possibility of a threat in the event of a scam caller. Moreover, the commission should require that foreign callers making telephone solicitations disclose that such calls originate from outside of the United States, further informing customers of the possibility of a scam.

- **The FCC should require that providers handle certain consumer transactions only at call centers located within the United States**. These transactions should include information relating to passwords, multi-factor authentication, social security numbers, or bank information — the types of information required to complete financial scams. The commission should also prohibit providers from making this type of information available at foreign call centers. These requirements would complicate scammers' efforts to access sensitive information while strengthening legal protections for customers by ensuring that they would have greater access to civil recourse in the event of a breach.

- **The FCC should prohibit providers from using call centers under the control or direction of "foreign adversary" nations**. While it is rare for call centers to be located in "foreign adversaries" — namely, Russia, China, North Korea, and Iran — foreign scam centers are often run by entities who likely receive direction or are influenced by these countries, particularly in Southeast Asia. As such, the commission should also ensure that any provider that wishes to operate a call center in any country complies with data security laws and practices at least as strong as those of the United States.

- **The FCC should apply its proposed regulations to "stand-alone" providers of non-interconnected VoIP and other internet-only providers**. Foreign scam centers often use a variety of methods to target victims, particularly as customers have modified their behavior or certain techniques become less effective due to crackdowns. As a result, the commission should seek to expand its regulations in a forward-leaning manner,

"Chinese Criminals Made More Than $1 Billion From Those Annoying Texts," *The Wall Street Journal*, October 14, 2025. (https://www.wsj.com/tech/cybersecurity/url-scam-texts-china-gangs-68e96097)

recognizing that scammers may shift their mode of communication and extortion in response to regulatory pressures.

- **The FCC should target foreign scam networks by requiring providers to post bond to file in the Robocall Mitigation Database**. The commission should require that providers post bond as an administrative incentive for firms to aggressively target scammers attempting to use their networks and resources as cover for illicit operations. Moreover, this broad-based approach eases compliance costs for the commission, saving the effort of having to select carve-outs or administer cutoffs in collecting payments from providers.

Conclusion

The commission can use its regulatory authority to shape the terrain that scammers must traverse to access American consumers, putting up barriers to accessing sensitive information while raising awareness among consumers of the risks posed by sharing certain types of sensitive information. The cost of inaction — measured in both dollars and national security risk — grows every day.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the commission's ongoing policy work.