Deputy Assistant Secretary David Bedard
for the Bureau of International Narcotics and Law Enforcement Affairs (INL)
Hearing with Senate Foreign Relations Committee on the SCAM Act
Written Testimony
August 6, 2026

Chairman Risch, Ranking Member Shaheen, and distinguished Members of the Committee, thank you for the opportunity to testify on the Department of State's work to protect Americans from criminal online scams.

U.S. losses to scam operations are staggering. They are hitting Americans in all 50 states, across every income level and age group. Our initial 2025 estimate of $12.5 billion in losses from Southeast Asia-based scams will likely rise considerably as we finalize our analysis. The threat is spreading into new regions and evolving operationally. Our response must be decisive and swift.

Although Burma, Cambodia, and Laos remain the epicenter, operations are expanding across Southeast Asia, South Asia, the Middle East, Africa, and the Pacific. The problem is compounded by global money laundering and human trafficking networks, inadequate screening of trafficking victims, and criminals exporting worldwide the tradecraft they refined in Southeast Asia.

The transnational criminal organizations behind these networks are also evolving quickly. As countries crack down, scammers are diversifying beyond large industrial-scale compounds into smaller, decentralized operations in hotels and residential areas that are harder for law enforcement to detect.

Chinese-origin transnational criminal organizations drive the Southeast Asia scam economy and run many of these operations. Their structure is more complex than a traditional criminal organization. They operate as loosely affiliated businesses with different specializations, all built to generate illicit revenue. Many are poly-criminal: running scams, trafficking drugs and people, and offering cybercrime as a service.

These organizations operate in distinct layers. At the top sits a leadership tier that colludes with government officials and builds out the criminal enterprise, often moving between jurisdictions on multiple citizenship-by-investment passports to evade accountability. Beneath them, a management tier runs the day-to-day scam operations, logistics, financial flows, and payoffs to local officials. Below them are scam workers of various nationalities. Many of them trafficking victims; others are willing participants. Across every layer sit the facilitators: complicit officials, lawyers, accountants, bankers, and cryptocurrency converters who keep this illicit economy running.

These networks exploit a persistent vulnerability: criminal operations are borderless, but law enforcement and legal authority stop at national borders. Criminals thrive in that gap. They base themselves in jurisdictions with weak legal frameworks, limited technical capacity, and often no established law enforcement cooperation channel with the United States, betting that fragmented national responses cannot keep pace.

INL is coordinating the Department of State's international response to implement President Trump's Executive Order 14390, Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens. The Executive Order focuses on three crime types (cybercrime, cyber-enabled fraud, and financially motivated sextortion). The bulk of current U.S. financial losses come from cyber-enabled fraud. State is working with the National Security Council and Homeland Security Council on an international approach built around four lines of effort:

First, a global diplomatic campaign, led by our regional bureaus, pressing key countries to act and holding those that do not accountable. This includes high-level demarches, joint statements, and coordinated messaging to governments harboring these operations. Our regional bureaus lead diplomatic engagement to build political will, while INL brings the connections to ministries of public security, interior, and justice, and to the law enforcement agencies that do the operational work. INL led the first-ever UN resolution on combating cyber fraud co-sponsored with Japan and the United Kingdom. In line with President Trump's Executive Order, this resolution calls upon all countries to thoroughly investigate

and prosecute fraud, target deceptive recruitment, and dismantle the financial networks and supply chains that organized criminal groups rely on to target Americans. INL will press countries to implement those commitments.

Second, imposing costs on transnational criminal organizations, their enablers, and the complicit officials who give them safe haven. Tools include visa restrictions, support for asset seizures, criminal indictments, extradition requests, and targeted sanctions to deny these networks resources and drive them to change their behavior. On July 23rd, Secretary Rubio announced a new visa restriction policy targeting cybercriminals, including those involved in scams and sextortion.

Third, advancing operational law enforcement cooperation and intelligence sharing. Where warranted, we provide training and equipment so foreign partners can investigate these criminal enterprises, their financial flows, and their enabling infrastructure. Thailand is a strong example. Over the last 18 months, INL has worked with Homeland Security Investigations to purposefully recruit Royal Thai Police officers with cyber, financial, and scam center expertise into positions within a partnership program called the Transnational Criminal Investigations Unit. This INL-backed program focuses on scam centers and related cyber-enabled crime affecting both our countries. Starting in October 2025, INL funded FBI deployments to Thailand following the evacuation of thousands of scam workers from compounds in Burma. Through INL, FBI, and HSI engagement with the Royal Thai Police, law enforcement agents are working in parallel with the Anti-Cyber Scam Center to support U.S.-nexus investigations. This gave U.S. law enforcement its first-ever opportunity to interview individuals emerging directly from scam compounds. FBI also worked with its Thai counterparts on U.S. investigative methods. The interviews and evidence transformed the U.S. Government's understanding of scam compound leadership, recruitment, coercion, financial operations, and tradecraft. FBI and Thai personnel also used INL-funded digital forensics tools to examine more than 8,000 mobile phones and 1,500 computer hard drives, corroborating witness testimony with digital evidence recovered directly from scam compounds. Our partnership with FBI and DOJ has supported multiple federal indictments and arrests targeting scam leaders and facilitators.

Fourth, prevention and outreach. This means engaging foreign executive and legislative counterparts, partnering with tech platforms to take down scam infrastructure, working with financial institutions to detect and block illicit transactions, and warning Americans through public awareness campaigns.

Together, these four lines of effort will deliver investigations, arrests, and prosecutions of cybercriminals who target Americans, and cut scam operations off from the enablers and infrastructure they depend on.

We appreciate the bipartisan interest in this issue and welcome the Committee's continued engagement as we implement the Executive Order. We look forward to working with you to protect Americans from these threats.

Thank you, and I welcome your questions.