Department of Justice

STATEMENT OF

KAREN P. SEIFERT
DIRECTOR, SCAM CENTER STRIKE FORCE
SPECIAL COUNSEL FOR NATIONAL SECURITY

UNITED STATES ATTORNEY'S OFFICE FOR THE DISTRICT OF COLUMBIA

BEFORE THE

JOINT ECONOMIC COMMITTEE
U.S. SENATE
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters

PRESENTED

March 25, 2026

STATEMENT OF
Karen P. Seifert
Director, Scam Center Strike Force
Special Counsel for National Security
United States Attorney's Office for the District of Columbia
U.S. Department of Justice

Before the
Joint Economic Committee
U.S. Senate
U.S. House of Representatives

At a Hearing Entitled
The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters

Presented
March 25, 2026

We are pleased to have the opportunity to share the work of the United States Attorney's Office for the District of Columbia (USAO-DC) to combat the growing threat of overseas scam compounds. President Trump has recognized the critical need to respond to cybercrime, as demonstrated through his Cyber Strategy for America and the issuance of Executive Order 14390. USAO-DC is proud to play a role in addressing this growing threat. Over the past few years, crypto investment fraud and other cyber-enabled internet confidence schemes have become an ever-rising tide of internet crime victimizing main street America. Elderly Americans' reporting of crypto currency scams has nearly doubled every year in the last four years,[1] and preliminary data indicates that in the last year alone, reported losses exceeded $17.7 billion. These scammers target Americans and use American infrastructure to perpetrate fraud. In Southeast Asia, one of the leading world hubs for scam activity, the scammers are organized in industrial scale compounds and guarded communities, wherein trafficked persons are held against their will and forced to participate in the scamming. These countries greatly benefit from the scams, with some reporting noting that as much as 40% GDP can be derived from scam revenue.[2] In Southeast Asia, the masterminds behind this $40 billion[3] per year industry are Chinese organized crime syndicates. This threat creates a generational wealth transfer from main street America to Chinese Transnational Organized Crime.

In response, last year, U.S. Attorney for the District of Columbia Jeanine Pirro launched the first-of-its kind "Scam Center Strike Force" (SCSF). The SCSF is a collaboration among USAO-DC, our partners at Main Department of Justice (Main DOJ), the Federal Bureau of

[1] *Internet Crime Report 2024*, Federal Bureau of Investigation Internet Crime Complaint Center 30, 35, *available at* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[2] *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*, United States Institute of Peace (May 2024), *available at* https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.
[3] *Id*.

Investigation (FBI), and the U.S. Secret Service, as well as, on select matters, the U.S. Postal Inspection Service, the Internal Revenue Service, and two other U.S. Attorney's offices. The SCSF focuses on investigating and disabling the worst scam centers operating in Southeast Asia, specifically in Cambodia, Burma, and Laos. The Strike Force's goals are to (1) seize and disable U.S. based infrastructure that is the manner and means of scam compound operations; (2) identify and charge the leaders of scam compounds, including Chinese organized crime affiliates, and seek to bring them to justice; (3) trace, seize, and forfeit the stolen cryptocurrency funds and return those funds to the American victims to the fullest extent permissible; and (4) prevent victimization through education of the public.

Scam Compounds in Southeast Asia

The work of the SCSF focuses on Southeast Asia, which is a hub of scam compound activity, with a multitude hosted in Burma, Cambodia, and Laos. The compounds often consist of a veritable "concentration camp" of scammers, where trafficked and enslaved persons are held against their will and beaten, forced into sex trafficking, or even killed if they do not make enough money off their victims. Many of these scammers respond to ads on U.S. social media platforms that advertise lucrative "jobs" to work at call centers in places such as Thailand. Upon arriving, however, they are shuttled over borders and held at compounds against their will. In the compounds, the trafficked victims are trained to scam and ordered to aim their efforts at American victims due to their wealth.

Scammers typically meet their American victims on social media, through platforms like Facebook, or text their victims, seemingly by mistake. They prey on older Americans' loneliness – gaining their trust and moving ongoing conversations over to WhatsApp and other encrypted communication channels. They then shuttle victims onto legitimate crypto platforms, only to convince them to move their crypto onto fake sites that the scammers control. Thus, these scam compounds connect to and use U.S. infrastructure, which is co-opted for criminal purposes, including: American social media companies used to recruit trafficked labor and meet U.S. victims; American satellite providers and VPN networks used to connect scam compounds to the internet; American data storage companies used to store scammers' training documents; American artificial intelligence companies used to determine the best methods to target victims; and American hosted .com websites, which appear more legitimate to U.S. users. These abuses of U.S. infrastructure and platforms degrade their reliability for the American people. The SCSF strategically works with private companies in the U.S. to prevent further abuse by cutting off access the scam centers' access to this infrastructure.

The masterminds behind the scam center operations, publicly reported to run the scam compounds in Southeast Asia and benefit from laundered crypto funds, are Chinese organized crime syndicates, enabled by lack of government regulation. For approximately 15 years, Chinese Transnational Crime Organizations (TCOs) have been establishing footholds in Southeast Asia for gambling schemes, after being pushed out of China due to the illegality of gambling in China. The TCOs have made substantial inroads in Burma, Laos, and Cambodia. Cyber scamming in Southeast Asia now generates more than $43.8 billion annually.[4] Reports from trafficked persons held in these compounds substantiate that, as the PRC has increased its

[4] *Id.*

efforts to stop scammers, the Chinese scam bosses have directed the scams be re-focused on American victims.

USAO-DC's Scam Center Strike Force

USAO-DC, under the leadership of U.S. Attorney Jeanine Pirro, is proud to have launched the SCSF, a first-of-its kind law enforcement initiative, to investigate the worst scam compounds in Southeast Asia. Launched in November 2025, the SCSF teams focus on identifying and pursuing key leaders—including Chinese organized crime affiliates operating in Cambodia, Laos, and Burma—to bring them to justice. USAO-DC, the prosecuting office in the nation's capital, has authority to charge foreign defendants and seize foreign property, and we are well-situated to engage with agencies across the government.

The SCSF combines the power, reach, and resources of USAO-DC with Main DOJ's Criminal Division, the FBI, and the U.S. Secret Service to disrupt these criminal schemes. In USAO-DC alone, approximately 10 Assistant U.S. Attorneys (AUSAs) are actively involved in investigation, prosecution, and management associated with the SCSF, along with about 5 support staff. USAO-DC AUSAs are supplemented by embedded Department of War staff and partner with 6 attorneys from Main DOJ's Criminal Division. The SCSF currently works with approximately 94 FBI agents, analysts, and managers from field office across the United States as well as FBI headquarters and partners with approximately 28 U.S. Secret Service agents and managers from field offices around the country. The SCSF also has collaborated on cases with the Internal Revenue Service, the U.S. Postal Inspection Service, and the U.S. Attorney's Offices in Rhode Island and the Western District of Washington. The SCSF seeks to use all government tools available, routinely partnering with the State Department, the Department of the Treasury's Office of Foreign Assets Control (OFAC), and the Department of Commerce.

We evaluate the SCSF's success in cases in numerous different ways. These include taking compounds offline, seizures of cryptocurrency, seizures of websites used to facilitate fraud, OFAC designations, and charging and prosecuting individuals who operate the scam centers. USAO-DC is extremely proud that in Fiscal Year 2024, USAO-DC helped seize $127,591,841.00, and in Fiscal Year 2025, USAO-DC helped seize $322,380,805.70.

Outside the U.S. government, the SCSF is working to develop collaboration with foreign partners. The SCSF is actively engaged in working with Southeast Asian countries and specifically has established connections with Thai law enforcement. In Bangkok, for example, the Strike Force has deployed FBI agents to embed with the Royal Thai Police War Room Task Force to combat scam compounds such as KK Park and compounds south of Min Lat Pan.[5] The Strike Force also worked with local police in Bali to investigate a network of scam centers. The suspects, directed by Cambodian-based organizers, targeted over 150 U.S. victims. The Strike Force's information was essential to the local prosecution of 38 Indonesian nationals.[6] The SCSF further continues to strengthen relationships among the Five Eyes and with Singapore. SCSF

[5] *New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans*; U.S. Attorney's Office for D.C. (Nov. 12, 2025), *available at* https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting.
[6] *Id.*

leadership is engaging with those partners to discuss how to increase coordination and refine efforts to exert maximum pressure on scam compound activity.

Additionally, the SCSF strategically collaborates with U.S. companies to combat this growing threat. The SCSF's efforts dovetail with the concerns of private industry about the use of their infrastructure for scamming and the way in which the same degrades trust in their networks. The SCSF is committed to working with private industry, including social media companies, satellite internet companies, and internet service providers to cut off access to the scam centers and prevent the use of U.S. infrastructure to perpetrate fraud against Americans.[7]

Beyond our work to combat scam centers, the SCSF is committed to educating Americans, especially older Americans, and their families about how to identify and not fall victim to these scams. We are collaborating with the U.S. Postal Inspection Service and private industry regarding public education and messaging. Further, U.S. Attorney Pirro has made public service announcements, given keynote speeches at conferences, and engaged the U.S. press to get the word out on this threat.

Need for Additional Authorities

On March 6, 2026, President Trump issued Executive Order 14390 "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens." Under this executive order, the National Coordination Center will create an operational cell, which will be responsible for coordinating federal efforts to detect, disrupt, dismantle, and deter cyber-enabled criminal activity conducted by foreign TCOs and associated networks that target United States persons, businesses, critical infrastructure, or public services. USAO-DC is working with our partners to implement the President's Executive Order and the President's Cyber Strategy for America.[8] The support of Congress in the form of resources and addressing gaps in the law will allow us to continue and expand these critical law enforcement operations.

Two specific gaps in the law currently impact the work of the SCSF. First, the SCSF would seek to prosecute non-U.S. nationals for human trafficking or forced labor for the purpose of committing wire fraud on U.S. persons. However, the relevant statutes make prosecution of extraterritorial non-U.S. nationals challenging. These same individuals who are using forced labor to commit wire fraud cannot be held accountable for the human trafficking occurring in their scam center compounds. Second, current law does not authorize the seizure and forfeiture of property used as an instrumentality of fraud, although in other contexts (e.g., terrorism), the law authorizes the seizure of the instruments of the crime. As a result, the U.S. government cannot seize websites used to perpetrate fraud based on the fraud alone. Rather, the government must further demonstrate that the website is involved in money laundering, which creates challenges obtaining warrants quickly to take down websites facilitating fraud on U.S. citizens.

---

[7] To preserve future cooperation and prevent bad actors from understanding the scope of cooperation and adjusting their practices, the U.S. Attorney's Office does not reveal the nature and extent to which companies voluntarily work with law enforcement. However, Meta, Google, and Microsoft have stated publicly that they are working with the SCSF.

[8] President Trump's Cyber Strategy for America (March 2025) *available at* https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

Accomplishments of the Scam Center Strike Force

USAO-DC is proud to have had several significant successes in combating these scam center compounds. The following are just a few examples of the SCSF's work.

The Scam Center Strike Force Burma team identified the Democratic Karen Benevolent Army (DKBA), a Burmese armed group and a belligerent in Burma's ongoing civil conflict, as supporting scam centers in Burma. We then took action against the DKBA scam centers. At the Tai Chang compound, we seized websites being used by the facility to victimize Americans, and at the 3 Pagodas Pass compound, we seized the Starlink terminals and accounts being used by the perpetrators to connect to the internet. We also nominated DKBA for designation by the Treasury Department, and in November 2025, the Treasury Department's OFAC sanctioned DKBA, a Burmese armed group, along with four of its senior leaders, for supporting cyber scam centers in Burma that target Americans using fraudulent investment schemes. OFAC also designated two foreign companies and Thai national Chamu Sawang, whom it linked to Chinese organized crime and stated worked with the DKBA and other armed groups to develop these scam centers.

In November and December 2025, the SCSF seized multiple web domains used by scams linked to the Tai Chang scam compound in Burma. The scammers used these web domains to connect victims to other platforms used to defraud them, and one seized domain was disguised as a legitimate investment platform to trick victims into unknowingly depositing their funds, showing fraudulent returns on what they believed to be their investments.[9]

USAO-DC, along with its partners, has filed numerous civil forfeiture complaints related to cryptocurrency frozen and seized from perpetrators in these schemes. For instance, in 2025, USAO-DC, along with Main DOJ's Computer Crime and Intellectual Property Section, filed a civil forfeiture complaint in the District of Columbia against over $225.3 million in cryptocurrency. The complaint alleges ties to cryptocurrency confidence schemes perpetrated from Southeast Asia. This represents the largest seizure of cryptocurrency ever made by the FBI and the Secret Service. The Department held a press conference about the complaint and used the opportunity to raise awareness about the threat and educate the public.[10]

* * *

We appreciate the opportunity to provide this information about the important work of the SCSF and our partners to respond to the growing threat of overseas scam compounds.

---

[9] *New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans*, U.S. Attorney's Office for D.C. (Nov. 12, 2025), *available at* https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting; *Justice Department Announces Seizure of Tai Chang Scam Compound Domain Used in Cryptocurrency Investment Fraud*, U.S. Department of Justice (Dec. 2, 2025), *available at* https://www.justice.gov/opa/pr/justice-department-announces-seizure-tai-chang-scam-compound-domain-used-cryptocurrency.

[10] *United States Files Civil Forfeiture Complaint Against $225M in Funds Involved in Cryptocurrency Investment Fraud Money Laundering*, U.S. Department of Justice (June 18, 2025), *available at* https://www.justice.gov/opa/pr/united-states-files-civil-forfeiture-complaint-against-225m-funds-involved-cryptocurrency.

USAO-DC and U.S. Attorney Jeanine Pirro are proud to have launched this first-of-its kind law enforcement initiative to investigate the worst scam compounds in Southeast Asia, and we look forward to continuing this critical work with your support.