Department of Justice

STATEMENT FOR THE RECORD
RICHARD GOLDBERG
ASSOCIATE COUNSEL
CRIMINAL DIVISION

BEFORE THE
JOINT ECONOMIC COMMITTEE

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

PRESENTED

March 25, 2026

Statement for the Record
Richard Goldberg
Associate Counsel
Criminal Division

Before the Joint Economic Committee

At a Hearing Entitled
"Overseas Scam Compounds in Southeast Asia"

Presented
March 25, 2026

Cryptocurrency investment fraud schemes have been growing at an alarming rate for years, victimizing Americans in every part of the country. One leading blockchain analysis platform estimates that $17 billion was stolen globally in cryptocurrency scams in 2025. In the U.S., our statistics come from victim reports filed with the FBI's Internet Crime Complaint Center or IC3. In 2024, IC3 recorded over $5.8 billion in loss to cryptocurrency investment fraud. That is more than a third of the total $16.6 billion in losses from all reports filed with IC3. Year-over-year growth in cryptocurrency victimization shows a 154% increase in number of complaints and a 92% increase in reported losses.

The Department of Justice and its federal law enforcement and agency partners are more focused than ever on dismantling the transnational criminal organizations responsible for causing the unprecedent billions of dollars in losses to American victims.

On March 6, 2026, the President issued an executive order that directly addresses this threat, entitled "Combatting Cybercrime, Fraud, and Predatory Schemes Against American Citizens." Through this EO, President Trump is unleashing every available tool to stop foreign-backed criminal networks that exploit vulnerable Americans through cyber-enabled fraud and extortion. It also seeks to incorporate additional tools to disable scam infrastructure. In sum, the U.S. will not simply play defense; the nation will use its offensive capacity to dismantle the organized crime groups at the heart of these scams.

Overview of the Scams

Where does cryptocurrency investment fraud originate? Southeast Asia is a hub of this scam activity, with Burma, Cambodia, and Laos hosting large-scale compounds devoted to fraud. The compounds often are filled with trafficked and enslaved persons held against their will who are beaten if they do not make enough money from their victims or try to escape. Many of these captives were fooled by advertisements on U.S. social media platforms, taking lucrative "jobs" to work at call centers in places such as Thailand. Upon arriving, however, they are shuttled over borders and held against their will.

In the compounds, the trafficked victims are trained to scam and ordered to target American victims to steal their wealth. If they refuse, or do not make enough money in the scam, they are sometimes forced to be sex workers, tortured, and even killed. The masterminds behind these operations, who are publicly reported to be running the scam compounds in Southeast Asia and benefitting from the laundered funds, are believed to be Chinese organized crime syndicates, enabled by lack of government regulation in country.

Scammers use sophisticated means to target U.S. citizens. They typically meet their American victims on social media, through platforms like Facebook, or text their victims, seemingly by mistake. They prey on Americans' loneliness. After gaining victims' trust, they move ongoing conversations over to WhatsApp and other encrypted communication channels. They shuttle their victims onto legitimate cryptocurrency platforms, only to then convince them to move their cryptocurrency to addresses controlled by the criminals, as directed on fake sites and apps that the scammers control.

These scam compounds also exploit U.S. infrastructure and U.S. platforms, which they co-opt for criminal purposes. For example, these criminal organizations use:

- American social media companies to recruit human trafficked labor and to target U.S. victims;
- American satellite providers and VPN networks to connect the scam compounds to the internet;
- American data storage companies to store scammers' training documents;
- American AI companies to determine the best methods to target their U.S. victims, and what conversations are most likely to spark interest; and
- American hosted domains, like .com websites, which appear more legitimate to U.S. users.

All of these efforts degrade consumer trust in U.S. infrastructure and U.S. platforms for the American people.

Even more importantly, the scam compounds engaged in cryptocurrency investment schemes are engaged in a massive transfer of generational wealth from everyday Americans into the hands of Chinese organized crime syndicates. They must be stopped.

The U.S. Response

Over the past several years, the Department of Justice has substantially increased its fight against cryptocurrency investment fraud schemes, the scam compounds that perpetrate such crimes, and the networks that launder their fraud proceeds.

Many Department components and U.S. Attorney's Offices across the country have brought complementary cases against Southeast Asian scam center operators and facilitators. One sterling example is the Scam Center Strike Force conceived and founded by the D.C. U.S. Attorney's Office, under the leadership of U.S. Attorney Jeanine Pirro. The Department's

Criminal Division, including the Computer Crime and Intellectual Property Section (CCIPS), the Fraud Section, and the Money Laundering, Narcotics and Forfeiture Section (MNF), partners with the United States Attorney's Office in the Strike Force.

The Strike Force's goals are to: (1) seize and disable U.S.-based infrastructure that are the manner and means of scam compound operations; (2) identify and charge the leaders of scam compounds, including the 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 and publicity around these actions.

The Strike Force works with public and private partners to accomplish its goals. For example, the Strike Force will share information, as appropriate, with the State Department, the Department of the Treasury's Office of Foreign Assets Control (OFAC), and the Department of Commerce as these agencies consider sanctions against criminal actors operating these compounds.

The Strike Force and the Department's Criminal Division as a whole have been strategically engaging with U.S. companies regarding this threat. Their efforts dovetail with private industry concerns over the use of their infrastructure to scam victims, and how that degrades trust in their networks. In many instances, the providers are able to cut off access to the scam centers and prevent U.S. infrastructure from being used as a means to perpetrate fraud against Americans.

The Strike Force is doing superb work fighting the battle against scam centers, but it is not acting alone. For example, in October 2025, the Department's National Security Division and the United States Attorney's Office for the Eastern District of New York unsealed an indictment charging PRC/Cambodian national Chen Zhi, the founder and chairman of Prince Holding Group, a multinational business conglomerate based in Cambodia, with wire fraud conspiracy and money laundering conspiracy for directing Prince Group's operation of forced-labor scam compounds across Cambodia.

Concurrently, in October 2025, the Department announced that it had seized and commenced forfeiture proceedings against bitcoin then-valued at approximately $15 billion, representing the criminal proceeds and instrumentalities of defendant Chen Zhi's fraud and money laundering schemes. That was the largest cryptocurrency seizure, ever.

Also in October 2025, at the same time as the Department's action against Chen Zhi and the Prince Group, OFAC announced sanctions against 146 targets within the Prince Group Transnational Criminal Organization, including sanctions against Chen Zhi, his close associates and business partners, and numerous Prince Group-affiliated corporate entities.

The Justice Department's Criminal Division also has brought charges against criminal syndicates responsible for laundering the proceeds of crypto investment scams. For example, during the past two years, eight defendants have pleaded guilty in federal court in Los Angeles for their roles in laundering more than $36.9 million stolen from victims of an international

digital asset investment scam conspiracy that was carried out from scam centers in Cambodia. The defendants include two Chinese nationals, one of whom managed a network of U.S.-based money launderers. In September 2025, one defendant was sentenced to 51 months of imprisonment. This case was prosecuted by the Criminal Division's Computer Crime and Intellectual Property Section, Fraud Section, and the U.S. Attorney's Office for the Central District of California.

Additional matters filed across the country recently include:

- In February, federal law enforcement working with the Eastern District of North Carolina seized $61 million of cryptocurrency tied to cryptocurrency investment fraud.
- A Chinese national was charged in the Eastern District of Texas with participating in a scheme to launder the proceeds of cryptocurrency investments scams involving millions of dollars in victim funds.
- A team of prosecutors and agents in the Central District of California obtained seizure warrants for over $112 million in funds linked to cryptocurrency investment schemes.
- Prosecutors in the Eastern District of Virginia and Northern District of New York obtained seizure warrants for numerous domain names used in cryptocurrency investment scams.
- Prosecutors in the District of Massachusetts have brought a series of civil forfeiture complaints to recover cryptocurrency involved in fraud schemes targeting Americans, including most recently a $3.4 million action filed in March.

The Department of Justice is also working closely with foreign law enforcement to counter this threat. In partnership with the State Department, the Justice Department operates the U.S. Transnational and High-Tech Crime Global Law Enforcement Network, or GLEN for short. Funded by State's Bureau of International Narcotics and Law Enforcement Affairs and run by the Justice Department's Criminal Division, the GLEN assigns experienced federal prosecutors overseas to advise and assist foreign countries on their investigations and prosecutions of cybercrime, intellectual property offenses, and related transnational organized crime. International Computer Hacking and Intellectual Property (ICHIPS) prosecutors based in Kuala Lumpur and Hong Kong will continue to play a key role in the Department's work to drive action on the ground in Southeast Asia against this threat.

Moreover, the Department's Office of International Affairs works with partners throughout Southeast Asia and around the world to arrest and extradite perpetrators and to obtain evidence for use in U.S. criminal investigations and prosecutions and share evidence in the U.S. for use in foreign investigations and prosecutions. A Department of Justice Attaché, based in Manila, Philippines, works directly with partners throughout Southeast Asia on operational matters to secure this assistance. Similarly, the FBI has deployed FBI agents to embed with the Royal Thai Police War Room Task Force to combat scam compounds in the region.

The Department of Justice is unwavering in its commitment to halt cyber-enabled scams. With the recently issued Executive Order entitled "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens," we are confident that all components of the federal government will join together to achieve maximum disruption of Southeast Asian scam centers to combat cybercrime, fraud, and predatory schemes against Americans. 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. The Department is committed to assisting the agencies tasked with implementing the President's Executive Order, and the President's Cyber Strategy for America.[2]

We thank Congress for bringing attention to this problem and look forward to discussing ways that, together, we can enhance the nation's capacity to achieve justice for victims and prevent harm to additional Americans.

[2] President Trump's Cyber Strategy for America, March 2025, see https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.