U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

The Honorable JD Vance
President
United States Senate
Washington, DC 20510

Dear President Vance:

On behalf of the Administration, we are pleased to present for congressional consideration a legislative proposal that would fix a gap in existing law and allow the seizure and forfeiture of property used as an instrumentality of fraud. The growing problem of overseas scam compounds was discussed at the recent Joint Economic Committee hearing, "The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters." This proposal is designed to permit the prompt take down, seizure, and forfeiture of instrumentalities of fraud, including the websites that facilitate the wire fraud committed from overseas scam compounds.

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.

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 websites that the scammers control. Thus, these scam compounds connect to and use U.S. infrastructure, which is co-opted for criminal purposes. In Southeast Asia, the masterminds behind this $40 billion[2] per year industry are Chinese organized crime syndicates. This threat creates a generational wealth transfer from main street America to Chinese Transnational Organized Crime.

[1] Fed. Bureau of Investigation Internet Crime Complaint Center, Internet Crime Report 2024, 30, 35 (2024) *available at* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[2] United States Institute of Peace, Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security (May 2024).

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 the U.S. Attorney's Office for the District of Columbia, Main Department of Justice (Department), the Federal Bureau of Investigation, 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. Attorneys' 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.

Currently, however, the SCSF and the Department more broadly face obstacles to swiftly take down the scam center websites used to perpetrate this fraud. 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 additional burdens on law enforcement to investigate and prove complicated money laundering schemes, as well as challenges obtaining warrants quickly to take down websites facilitating fraud on U.S. citizens. In addition, the government faces similar additional challenges when seeking to forfeit other property the criminals use to facilitate fraud, to disrupt criminal activity, and increase recoveries for victims.

The Department of Justice offers this proposed amendment to provide a necessary tool to combat the fraud committed in overseas scam centers. This bill amends Federal forfeiture provisions under 18 U.S.C. § 981 to permit the seizure and forfeiture of property used as an instrumentality of fraud.

By making these changes to Section 981, the bill authorizes the seizure and forfeiture and would allow for the prompt take-down of the websites scammers use to commit wire fraud occurring in overseas scam center compounds. It would also allow the seizure and forfeiture of additional property to take the tools of the trade away from scammers and to compensate victims. The Department looks forward to working with Congress on this legislative action.

Sincerely,

PATRICK DAVIS

Digitally signed by PATRICK DAVIS
Date: 2026.09.09 11:28:04 -04'00'

Patrick D. Davis
Assistant Attorney General

Enclosure