

October 21, 2025

DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks, Underscoring Cyber-Enabled Fraud as an Enforcement Priority

On October 14, 2025, the Department of Justice (DOJ), the Department of Treasury's Office of Foreign Assets Control (OFAC), and Treasury's Financial Crimes Enforcement Network (FinCEN) announced significant enforcement actions against Southeast-Asian scam networks targeting Americans through "pig butchering" cryptocurrency investment schemes and other types of fraud.

In announcing DOJ's indictment and record-setting \$15 billion forfeiture action, Attorney General Pam Bondi stated: "Today's action represents one of the most significant strikes ever against the global scourge of human trafficking and cyber-enabled financial fraud."¹ Similarly, in announcing the Treasury actions, Secretary of the Treasury Scott Bessent stated: "The rapid rise of transnational fraud has cost American citizens billions of dollars, with life savings wiped out in minutes. Treasury is taking action to protect Americans by cracking down on foreign scammers . . . Treasury will continue to lead efforts to safeguard Americans from predatory criminals."²

These enforcement actions reflect the increased focus on cyberfraud as an enforcement priority, as reflected in recent statements by the DOJ and FinCEN.³ In this memorandum, we consider these actions in greater detail and discuss practical steps financial institutions may wish to take.

¹ U.S. Dep't of Just., *Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025), available [here](#).

² U.S. Dep't of Treasury, *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025), available [here](#).

³ In Congressional testimony in September 2025, FinCEN Director Andrea Gacki noted that FinCEN was prioritizing combatting fraud and cyber scams. *See* U.S. Dep't of Treasury, FinCEN, *Statement by Andrea M. Gacki before the Committee on Financial Services' Subcommittee on National Security, Illicit Finance, and International Financial Institutions* (Sep. 9, 2025), available [here](#). In May 2025, the DOJ's criminal division announced enforcement priorities, which included "[f]raud that victimizes" Americans such as "elder fraud." U.S. Dep't of Just., *Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime 4* (May 12, 2025), available [here](#). In June 2025, the U.S. Attorney's Office for the District of Columbia announced a civil forfeiture complaint for more than \$225 million for cryptocurrency connected to the theft and laundering of funds from cryptocurrency investment fraud schemes. *See* U.S. Dep't of Just., *Largest Ever Seizure of Funds Related to Crypto Confidence Scams* (June 18, 2025), available [here](#).

Department of Justice: Indictment and Forfeiture Action

The U.S. Attorney’s Office for the Eastern District of New York (EDNY) charged Chen Zhi, founder and chairman of Prince Holding Group (Prince Group), with operating forced-labor camps across Cambodia that perpetrated fraudulent cryptocurrency investment schemes. United States Attorney Joseph Nocella Jr. called the Prince Group’s scheme “one of the largest investment fraud operations in history.”⁴

According to DOJ, trafficked workers were coerced into executing “pig butchering” scams, which involved gaining victims’ trust online, sometimes through romantic scams, and then deceiving them into investing in fake crypto assets. The Prince Group targeted victims around the world, including in the United States, with assistance from various local networks. One such network in Brooklyn laundered about \$18 million of illicit proceeds from over 250 American victims between May 2021 and August 2022.⁵ Prince Group executives bribed foreign officials and laundered proceeds through seemingly legitimate businesses. Its associates employed sophisticated techniques like “spraying” and “funneling” to obscure the transaction history of its ill-earned profits, fragmenting large volumes of cryptocurrency and consolidating funds back into fewer virtual currency addresses.⁶

The DOJ’s National Security Division and EDNY also initiated a civil in rem forfeiture action seeking approximately 127,271 bitcoin, worth about \$15 billion, from proceeds and instrumentalities of the fraud and money laundering schemes. This marks the largest forfeiture action DOJ has ever pursued.⁷ Some of these proceeds were held in wallets at cryptocurrency exchanges or converted into fiat currency stored in traditional bank accounts.⁸ Other proceeds were stored in unhosted cryptocurrency wallets controlled by Chen Zhi.⁹

OFAC: Transnational Criminal Organization Designations

OFAC sanctioned 146 individuals and entities associated with the Prince Group, including Chen Zhi, placing them on OFAC’s Specially Designated Nationals and Blocked Persons List.¹⁰ These designations were made under OFAC’s transnational criminal organization authorities. OFAC noted that the Prince Group operates at least ten “scam compounds” in Cambodia, including those operated by the Jin Bei Group, which had been linked to “reports of extortion, scamming, forced labor, and the gruesome murder of a 25-year-old Chinese national[.]”¹¹ OFAC described Cambodia as the center of the Prince Group’s operations, but other designations targeted its offshore hubs and shell companies in Singapore, Palau, the Cayman Islands, the British Virgin Islands, Hong Kong, and Taiwan.¹²

In parallel, the U.K.’s Office of Financial Sanctions Implementation (OFSI), added 12 individuals and entities associated with the Prince Group to the U.K. Sanctions List.¹³ This coordinated effort follows a January 2025 memorandum of understanding executed between OFAC and OFSI.

These designations follow other recent OFAC designations of Southeast Asian individuals and entities for cyber scam operations that target Americans.¹⁴

⁴ U.S. Dep’t of Just., *Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025), available [here](#).

⁵ Indictment at ¶ 44, *U.S. v. Chen Zhi*, No. 1:25-cr-00312 (E.D.N.Y. Oct. 8, 2025).

⁶ U.S. Dep’t of Just., *Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025), available [here](#).

⁷ *Id.*

⁸ Complaint at ¶ 52, *In re Approximately 127,271 Bitcoin (“BTC”) Previously Stored at the Virtual Currency Addresses Listed in Attachment A, And All Proceed Traceable Thereto*, No. 1:25-cv-05745 (E.D.N.Y. Oct. 14, 2025).

⁹ *Id.*

¹⁰ U.S. Dep’t of Treasury, *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025), available [here](#).

¹¹ *Id.*

¹² *Id.*

¹³ U.K. Office of Financial Sanctions Implementation HM Treasury, *Financial Sanctions Notice* (Oct. 8, 2025), available [here](#).

¹⁴ The actions follow OFAC’s designations of Burmese and Cambodian cyber scam facilitators on September 8, Burmese Warlord Saw Chit Thu on May 5, and Philippines computer infrastructure company Funnall Technology Inc. on May 29. See U.S. Dep’t of Treasury, *Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams* (Sept. 8, 2024), available [here](#); U.S. Dep’t of Treasury, *Treasury Sanctions Burma Warlord and Militia Tied to Cyber*

FinCEN: Section 311 Final Rule

FinCEN finalized a rule under section 311 of the USA PATRIOT Act, effectively severing Huione Group, a Cambodia-based financial services conglomerate, from the U.S. financial system.¹⁵ FinCEN determined that Huione Group has served as a critical node for transnational criminal organizations in Southeast Asia and illicit actors from the Democratic People's Republic of Korea, laundering over \$4 billion of illicit proceeds between August 2021 and January 2024. The final rule prohibits U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for, or on behalf of, Huione Group.¹⁶ U.S. financial institutions must implement risk-based procedures and screening to identify and block transactions involving Huione.¹⁷

Key Takeaways

The DOJ, OFAC, and FinCEN's recent enforcement actions reflect the U.S. government's heightened focus on international cyber-enabled fraud and scams targeting Americans and associated money laundering.¹⁸ This issue has taken on increasing significance across the federal government, and has been a recent focus of the federal banking agencies.¹⁹ Financial institutions should consider taking additional proactive steps to review and enhance their controls to mitigate the risks associated with such illicit activity, if necessary. Among other things, financial institutions should consult relevant FinCEN advisories, including a September 2023 alert on "pig butchering" that contains behavioral red flags, financial red flags, and technical red flags.²⁰

Scam Operations (May 5, 2025), available [here](#); U.S. Dep't of Treasury, *Treasury Takes Action Against Major Cyber Scam Facilitator* (May 29, 2025), available [here](#).

¹⁵ Though it was announced on October 14, the final rule was issued on October 15. U.S. Dep't of Treasury, FinCEN, *FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System* (Oct. 15, 2025), available [here](#). The proposed rule had been announced in May 2025. U.S. Dep't of Treasury, FinCEN, *FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists* (May 1, 2025), available [here](#).

¹⁶ U.S. Dep't of Treasury, FinCEN, *FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System* (Oct. 15, 2025), available [here](#).

¹⁷ *Id.*; see also U.S. Dep't of Treasury, *FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System* (Oct. 15, 2025), available [here](#).

¹⁸ The private and nonprofit sector have increasingly focused on fraud and scams as a national security crisis. See Aspen Institute, *United We Stand: A National Strategy to Prevent Scam* 6 (Sept. 30, 2025), available [here](#) ("This epidemic of fraud is a multi-pronged threat to national security and the livelihood of all Americans. As transnational criminals siphon billions of dollars from Americans, they empower their own criminal, authoritarian, or terrorist ambitions while undermining the financial security of millions of U.S. households. This fuels insecurity and erodes trust in America's core systems of government, commerce, and communication.").

¹⁹ U.S. Dep't of Treasury, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation, *Request for Information on Potential Actions to Address Payments Fraud* (June 13, 2025), available [here](#).

²⁰ U.S. Dep't of Treasury, *FinCEN Issues Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (Sept. 8, 2023), available [here](#).

**DOJ and Treasury Undertake Significant Enforcement Actions Targeting Southeast Asian Scam Networks,
Underscoring Cyber-Enabled Fraud as an Enforcement Priority**

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jessica S. Carey

+1-212-373-3566

jcarey@paulweiss.com

John P. Carlin

+1-202-223-7372

jcarlin@paulweiss.com

Roberto J. Gonzalez

+1-202-223-7316

rgonzalez@paulweiss.com

Elizabeth Hanft

+1-212-373-3664

ehanft@paulweiss.com

Brad S. Karp

+1-212-373-3316

bkarp@paulweiss.com

David K. Kessler

+1-212-373-3614

dkessler@paulweiss.com

Loretta E. Lynch

+1-212-373-3000

Mark F. Mendelsohn

+1-212-373-3337

mmendelsohn@paulweiss.com

Ian C. Richardson

+1-202-223-7405

irichardson@paulweiss.com

Jacobus J. Schutte

+1-212-373-3152

jschutte@paulweiss.com

Nicole Succar

+1-212-373-3624

nsuccar@paulweiss.com

Benjamin Klein

+1-202-223-7317

bklein@paulweiss.com

Samuel Kleiner

+1-212-373-3797

skleiner@paulweiss.com

Associates Charlotte G. Cooper and Liliana Ramirez contributed to this Client Memorandum.