DOJ's Crypto Fraud Strike Force: Implications for Digital Asset Platforms and Intermediaries

November 25, 2025

On November 12, 2025, the U.S. Department of Justice ("DOJ") announced the launch of a cross-agency strike force targeting the type of cryptocurrency-related scam known as pig butchering.[1] For companies involved in digital asset transactions, this enforcement initiative carries certain compliance implications.

The "Scam Center Strike Force," based out of the U.S. Attorney's Office for the District of Columbia, in collaboration with DOJ's Criminal Division, the FBI and the U.S. Secret Service, is focused on transnational criminal organizations based in Southeast Asia, many with links to Chinese organized crime and human trafficking. DOJ announced that the strike force is "already up and running," has seized and forfeited nearly $402 million in cryptocurrency to date and recently filed another $80 million forfeiture proceeding. DOJ also announced that the strike force would partner with the State Department, the Treasury Department's Office of Foreign Assets Control ("OFAC") and the Commerce Department, reflecting a whole-of-government approach with a focus on both U.S. and foreign targets.

At the same time as this announcement, OFAC imposed new sanctions on a Burma-based armed group—the Democratic Karen Benevolent Army ("DKBA")—and related actors based on their role in operating scam compounds.[2] These coordinated actions underscore that these schemes are being treated not only as fraud and money-laundering crimes but also as significant national security concerns.[3]

---

1 Press release, *New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans*, https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting (Nov. 12, 2025).

2 Press release, *Treasury Sanctions Burma Armed Group and Companies Linked to Organized Crime Targeting Americans*, https://home.treasury.gov/news/press-releases/sb0312 (Nov. 12, 2025).

3 DOJ's strike force announcement builds on related measures taken recently by the Financial Crimes Enforcement Network ("FinCEN") to counter pig butchering schemes. *See, e.g.*, FinCEN, FIN-2023-Alert005, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as Pig Butchering,*

Below, we provide an overview of pig butchering schemes and discuss the compliance-related implications of the new strike force for exchanges and other intermediaries involved in digital asset transactions.

Pig Butchering Schemes. In a typical pig butchering scheme, a scammer operating from a foreign jurisdiction with a fake online identity will send a text or social media message to a target to try to establish a trusting relationship. The scammer will build a rapport with the victim, eventually encouraging the victim to make an "investment," typically in a digital asset. Once the victim has transferred the funds, the perpetrator cuts off all contact and moves the funds to different accounts or crypto wallets. These schemes are, at bottom, sophisticated social engineering attacks, much like many modern cyber intrusions. Scammers call the practice pig butchering because they compare it to fattening hogs before slaughter.[4]

Pig butchering is a lucrative global enterprise. According to DOJ's announcement, these schemes generate billions of dollars in illicit profits every year and are often perpetrated by groups operating in Southeast Asia. The scams typically involve a degree of sophistication. For example, after convincing a victim to transfer the so-called investment, the perpetrators often launder the assets by moving them through a series of anonymous addresses and ultimately depositing them at an exchange.

According to DOJ and press reports, criminal organizations have set up entire compounds—sometimes staffed by victims of human trafficking—focused solely on

---

https://www.fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf (Sept. 8, 2023); FinCEN, *Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern*, 90 Fed. Reg. 48295 (Oct. 16, 2025) (prohibiting access to U.S. financial system for group laundering illicit proceeds from, *inter alia*, cryptocurrency investment scams carried out by Southeast Asian criminal organizations); *see also* Press release, *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia*, https://home.treasury.gov/news/press-releases/sb0278 (Oct. 14, 2025); Press release, *Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams*, https://home.treasury.gov/news/press-releases/sb0237 (Sept. 8, 2025); Press release, *Treasury Takes Action Against Major Cyber Scam Facilitator*, https://home.treasury.gov/news/press-releases/sb0149 (May 29, 2025); Press release, *Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations,* https://home.treasury.gov/news/press-releases/sb0129 (May 5, 2025).

[4] *See* FIN-2023-Alert005 *supra*. Several outlets have reported recently on investigations revealing the extensive scale and reach of pig butchering and related crypto fraud. *See* The New York Times; Wired Magazine; and International Consortium of Investigative Journalists.

defrauding victims (often based in the United States) and laundering the proceeds. OFAC sanctioned DKBA for its alleged role in such conduct.

Compliance Implications for Digital Asset Firms. With expanded law enforcement efforts to detect and prosecute pig butchering schemes, crypto platforms and intermediaries should expect heightened scrutiny and expectations from regulatory and enforcement authorities, particularly around anti-money laundering ("AML"), know-your-customer ("KYC"), and sanctions compliance. Depending on a firm's unique risk exposure, the following areas may warrant particular focus:

- **Monitoring for Red Flags.** Regulators may expect firms to implement risk-based procedures and controls to detect pig butchering, as applicable. For example, high-dollar transfers to newly created or thinly used wallets, rapid movement through mixers or high-risk chains, wallet exposure (even indirectly) to suspicious organizations in Southeast Asia, and indications of social engineering in on-platform communications may be among the factors that compliance systems should seek to detect. To the extent consistent with privacy laws, customer disclosures and other obligations, firms also may consider the use of advanced analytics and AI tools to identify patterns in account activity and communications consistent with pig butchering typologies.

- **Enhanced KYC.** Firms should also prepare for heightened regulatory expectations around new customer onboarding. Enhanced KYC diligence may be warranted where any indicia suggest potential links to accounts, wallets, organizations, IP addresses or regions tied to pig butchering. A number of blockchain analytics vendors (including TRM Labs, Chainalysis and Elliptic, for example) maintain databases of wallet addresses and clusters associated with known scams, sanctions targets and other illicit activity and offer screening tools to identify customer or transactional exposure to those addresses. Firms should evaluate the capabilities of their current analytics stack and consider whether additional data sources or vendor integrations would be appropriate.[5]

- **Sanctions Compliance.** As noted above, OFAC added DKBA and several related entities and individuals to its Specially Designated Nationals ("SDN") list, in addition to various prior designations related to involvement in pig butchering scams. As a result, U.S. persons are prohibited from engaging in any transactions with such sanctioned parties, and their assets in the possession or control of U.S. persons are blocked. Firms should, of course, update their sanctions compliance systems to

---

[5] *See also* NY Dep't of Financial Services, *Notice on Use of Blockchain Analytics for New York Banking Organizations* (Sept. 17, 2025), https://www.dfs.ny.gov/industry-guidance/industry-letters/il20250917-blockchain.

account for OFAC sanctions designations. As to existing customers, robust IP analytics and real-time sanctions rescreening may be warranted in addition to ongoing monitoring for transactional activity with a potential nexus to sanctioned parties.

- **Proactive Cooperation**. In announcing the new strike force, DOJ called for a "public-private partnership," asking U.S. firms to "partner in the initiative" in order to "secure the U.S. infrastructure." Federal law enforcement therefore may expect companies to proactively share intelligence with the U.S. government (beyond filing SARs), such as promptly reporting to law enforcement on suspicious activity patterns. Companies should ensure that any such proactive disclosures comport with relevant privacy laws. Relatedly, regulators increasingly may expect data sharing across market participants, such as proactively notifying other exchanges and intermediaries about suspicious wallets or IP clusters or new social engineering tactics.

- **Law Enforcement Requests**. Federal agencies will expect robust and speedy cooperation more generally. Platforms should prepare for an uptick in subpoenas and similar requests from federal law enforcement agencies. Regulators will likely expect market participants to have in place sophisticated procedures to process requests, preserve records, freeze wallets and accounts where authorized and produce responsive documents on short notice.

- **International Coordination**. Given the transnational nature of pig butchering schemes, U.S. agencies will seek to collaborate and partner with overseas counterparts on investigations and enforcement.[6] Digital asset firms should therefore expect greater regulatory scrutiny and requests in other jurisdictions as well. Similarly, when potential misconduct is identified, firms should carefully consider whether and how to notify any foreign government agencies.

* * *

In sum, the new strike force is a significant development, indicating an expansive multi-agency effort to investigate and prosecute the individuals, groups and entities that have allowed pig butchering schemes to proliferate. By connecting these crimes to transnational criminal organizations and sanctioned groups, DOJ is positioning this issue as a matter of national security, aligned with broader priorities of the Trump Administration. Thus, although DOJ has already been active in prosecuting crypto-

[6] *See, e.g., U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia, supra* n.3.

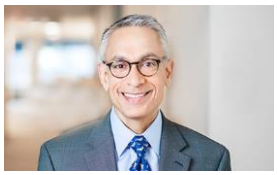
related fraud and money laundering over the past several months,[7] this announcement indicates that crypto enforcement will become better-resourced and more aggressive going forward. Digital asset firms operating in the United States should consider reviewing and making appropriate enhancements to their AML, KYC, and sanctions compliance policies and procedures in light of the increasing risk.

Please do not hesitate to contact us with any questions.

---

[7] *See, e.g.*, Press release, *Founder of Chicago Cryptocurrency Company Indicted in Alleged $10 Million Money Laundering Conspiracy*, https://www.justice.gov/usao-ndil/pr/founder-chicago-cryptocurrency-company-indicted-alleged-10-million-money-laundering (Nov. 18, 2025); Press release, *Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes*, https://www.justice.gov/usao-edny/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged (Oct. 14, 2025); Press release, *Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and other Assets*, https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets (Aug. 14, 2025); Press release, *OmegaPro Founder and Promoter Charged for Running Global $650M Foreign Exchange and Crypto Investment Scam*, https://www.justice.gov/opa/pr/omegapro-founder-and-promoter-charged-running-global-650m-foreign-exchange-and-crypto (Jul. 8, 2025); Press release, *Founder of Cryptocurrency Payment Company Charged with Evading Sanctions and Export Controls, Defrauding Financial Institutions, and Violating the Bank Secrecy Act*, https://www.justice.gov/opa/pr/founder-cryptocurrency-payment-company-charged-evading-sanctions-and-export-controls (June 9, 2025).

Andrew J. Ceresney
Partner, New York
+ 1 212 909 6947
aceresney@debevoise.com



Satish M. Kini
Partner, Washington, D.C.
+ 1 202 383 8190
smkini@debevoise.com

Douglas S. Zolkind
Partner, New York
+1 212 909 6804
dzolkind@debevoise.com

Aseel M. Rabie
Counsel, Washington, D.C.
+1 202 383 8162
arabie@debevoise.com

Eric Halliday
Associate, New York
+ 1 212 909 6911
eshalliday@debevoise.com