

SDNY Forfeiture Action Targets \$61 Million in Tether Linked to Iranian Oil Sales: Key Takeaways for Digital Assets

By Richard Weber, Brianne Wylie | October 20, 2026

RELATED PRACTICES White Collar and Investigations, Digital Asset and Cryptocurrency Litigation

The U.S. Attorney's Office for the Southern District of New York ("SDNY") filed a civil forfeiture complaint on Sept. 14, 2026, seeking approximately \$61 million in Tether (USDT) stablecoins. The U.S. government alleges the funds are proceeds of black-market sales of sanctioned Iranian oil intended to benefit the Iranian government and the Islamic Revolutionary Guard Corps ("IRGC"), a designated Foreign Terrorist Organization.

The case shows Department of Justice ("DOJ") using civil forfeiture to reach crypto held offshore, relying on stablecoin issuers to execute seizures, and combining sanctions, anti-money laundering ("AML") and counterterrorism tools against the digital asset sector. FBI Assistant Director in Charge James C. Barnacle, Jr. [is quoted saying](#) that this complaint "demonstrates the FBI's ability to follow the money, root out illicit schemes, and halt the stream of cryptocurrency to any government attempting to evade sanctions or committing terrorist activities."

Factual Summary

According to the complaint, two Hong Kong companies—Blessed Trust, posing as a wealth manager and crypto custodian, and Hexa Whale, posing as a commodities brokering company—used exchange accounts to "launder the proceeds of black-market sales of Iranian oil proceeds" into cryptocurrency and funnel the illicit funds to the Iranian government.

A linked network of unhosted cryptocurrency addresses known as "Entity A" allegedly moved more than \$1.5 billion, sending funds to IRGC-linked cryptocurrency addresses and an Iranian exchange. One wallet was reportedly used by Sepehr Energy, a sanctioned front company that manages and oversees Iran's military oil sales.

Critically, the alleged scheme touched the U.S. banking system: roughly \$480 million in wires to the two companies cleared through a correspondent account at a New York bank without OFAC licenses. Tether Limited, the company that manages the smart contracts and the funds held in reserve for USD Tether, froze the 10 target wallets in mid-2025. Under a court-issued seizure warrant, the frozen tokens—just under 61.2 million USDT—will be transferred to an FBI-controlled hardware wallet.

Key Legal Points

Civil *In Rem* Forfeiture vs. Criminal Forfeiture: The case is brought against the property itself, not any individual person or entity. Civil forfeiture generally requires no indictment or conviction and can reach assets of foreign actors beyond the government's personal jurisdiction. No one has been charged, and the complaint alleges no wrongdoing by the exchange or Tether.

Three Legal Theories: The complaint advances three independent bases for forfeiture. First, it alleges the funds are proceeds of Iran sanctions violations. Second, it alleges money laundering—that the funds were moved to promote unlawful activity and to conceal their source. Third, it invokes a terrorism theory, alleging the funds are assets of entities supporting the IRGC. This last theory is exceptionally broad, because it reaches all assets of such an entity and not just those traced to a specific offense.

Blockchain Tracing: The FBI linked the wallets to common control using public blockchain records—for example, one wallet funding or paying fees for another, an existing address being used to activate a new address or one address transferring all or a majority of its funds to another. Expect this kind of on-chain analysis to be central in future cases.

Why This Case Matters

The action signals several shifts in DOJ's posture toward digital assets. Most notably, DOJ now views stablecoins like USDT as a primary channel for sanctions evasion, given their liquidity and dollar stability. Proceeding civilly rather than criminally lets the government seize those funds with a lower burden of proof and without first indicting or extraditing foreign actors, making civil forfeiture a strategic tool.

The case also casts stablecoin issuers as de facto enforcement partners: issuers are now participants in seizures and should expect more law enforcement requests. At the same time, the case confirms that the dollar remains the jurisdictional hook. Despite the crypto assets at issue, U.S. reach ultimately rests on dollar wires that cleared through U.S. banks, and any transaction touching the dollar system is within reach.

Practical Takeaways for Clients

Crypto Exchanges and Virtual Asset Service Providers (VASPs): Exchanges and VASPs should screen at the wallet level using blockchain analytics, rather than simply checking names against OFAC lists, and should assess indirect exposure as well. Customers whose activity does not match their stated business warrant scrutiny. Platforms should have a documented protocol in place for responding to law enforcement freeze requests.

Stablecoin Issuers: Issuers should formalize their processes for responding to freeze, burn and seizure requests and document every action taken. Because freeze capability is now a recognized enforcement tool, issuers should also weigh its legal and reputational implications.

Financial Institutions and Correspondent Banks: Banks should monitor wires involving Hong Kong and UAE intermediaries—particularly those for crypto, commodities or petroleum-trading clients—for sanctions-evasion red flags. They should also recognize that dollar clearing alone can expose foreign transactions to U.S. forfeiture actions.

Trading and Commodity Firms: Trading firms should review their counterparty and payment-routing diligence for exposure to Iranian oil, including intermediaries whose profiles do not fit the trade. If gaps surface, firms should evaluate with counsel whether voluntary self-disclosure to OFAC or DOJ is warranted.

Individuals and Potential Claimants: Anyone whose assets are frozen or seized should act quickly: third parties can contest forfeiture, but the deadlines are short. Claimants should also

preserve all records relating to affected assets and consider any board reporting or disclosure obligations.

[See the complaint here.](#)