

White Collar Defense and Investigations



September 23, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorney or call your regular Skadden contact.

Ryan D. Junck

Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Andrew M. Good

Partner / London
44.20.7519.7247
andrew.good@skadden.com

Greg Seidner

Counsel / London
44.20.7519.7200
greg.seidner@skadden.com

Ahmed H. Ali

Associate / London
44.20.7519.7178
ahmed.ali@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

SDNY's \$61 Million Crypto Forfeiture Action Reflects Growing Convergence of Civil Forfeiture and Sanctions Enforcement

Executive Summary

- **What's new:** The SDNY U.S. Attorney's Office has filed a civil forfeiture complaint alleging that approximately \$61 million in USD stablecoin funds trace to black-market sales of sanctioned Iranian crude oil and petroleum products laundered through Hong Kong-incorporated firms.
- **Why it matters:** The action reflects an accelerating pattern of coordinated DOJ and Treasury enforcement that pairs civil forfeiture's lower evidentiary burden with expanding sanctions authority over digital assets, materially increasing exposure for non-U.S. exchanges, trading firms and digital asset issuers with even indirect Iran-linked flows.
- **What to do next:** Cryptocurrency exchanges and virtual asset service providers should consider implementing enhanced blockchain analytics, strengthening KYC and customer due diligence processes for high-risk counterparties and proactively engaging with digital asset issuers' compliance programs.

On September 14, 2026, the U.S. Attorney's Office for the Southern District of New York (SDNY) filed a civil forfeiture complaint seeking approximately \$61 million in a U.S. dollar (USD) stablecoin (the Complaint). Prosecutors allege the funds trace to black-market sales of sanctioned Iranian crude oil and petroleum products.¹

According to the government, two Hong Kong-incorporated firms — Blessed Trust Limited and Hexa Whale Trading Limited — used trading accounts at a cryptocurrency exchange based in the United Arab Emirates (UAE) to launder proceeds into a network that has moved more than \$1.5 billion to Iran's government and the Islamic Revolutionary Guard Corps (IRGC), a U.S.-designated terrorist organization.²

The action is the latest in an accelerating pattern of coordinated U.S. Department of Justice (DOJ) and U.S. Department of the Treasury enforcement that pairs civil forfeiture's lower evidentiary burden with expanding sanctions authority over digital assets — materially increasing exposure for non-U.S. exchanges, trading firms and digital asset issuers with even indirect Iran-linked flows.

¹ Press Release, U.S. Att'y's Office, S.D.N.Y., "U.S. Attorney Seeks Forfeiture of \$61 Million in Cryptocurrency From the Iranian Military's Black-Market Oil Sales" (Sept. 14, 2026).

² *Id.* (quoting Deputy U.S. Attorney Sean S. Buckley: "The Government of Iran used a network of cryptocurrency actors in China and elsewhere to launder more than \$1.5 billion in illicit oil money intended to benefit the Iranian military and the terror-designated IRGC.")

SDNY's \$61 Million Crypto Forfeiture Action Reflects Growing Convergence of Civil Forfeiture and Sanctions Enforcement

The Action Against Blessed Trust and Hexa Whale

The Complaint alleges that Blessed Trust and Hexa Whale each misrepresented the nature of their business to financial institutions and virtual-asset service providers. The former held itself out as a wealth-management and custodial firm, the latter as a commodities broker, the Complaint claims; in fact, they received and transferred the proceeds of Iranian crude oil and petroleum-product sales and provided fiat-to-crypto “on-ramp” services, including through U.S.-based cryptocurrency issuers.³

Blessed Trust and Hexa Whale clients included “Company-1,” a Hong Kong-incorporated company that purports to operate in the international petroleum market.

The government alleges that funds flowed through Blessed Trust and Hexa Whale’s exchange accounts to a cluster of at least seven interrelated unhosted “Entity A” wallets that have reportedly received and distributed more than \$1.5 billion in Iranian oil proceeds, including transfers to the Iranian exchange Nobitex and to Middle East money transmitters believed to be IRGC fronts.

The Complaint further alleges that Sepehr Energy, a U.S.-sanctioned Iranian front company that manages black-market oil sales on behalf of Iran’s Armed Forces General Staff, used one Entity A wallet as part of a terrorism-financing infrastructure it controls.

The forfeiture action identifies the U.S. dollar stablecoin held in 10 TRON-network wallets as the defendants *in rem*. According to the Complaint and likely upon DOJ outreach, the stablecoin issuer froze seven of the 10 wallets on June 15, 2025, and the remaining three on July 26, 2025, with individual balances ranging from roughly \$1 million to \$12.76 million.

Because the action is civil, the government need only prove its case by a preponderance of the evidence rather than meet the higher criminal standard. Indeed, no criminal conviction, and no U.S.-person defendant, is required.

The complaint alleges that the defendant USD stablecoin constitutes:

- Proceeds traceable to an International Emergency Economic Powers Act (IEEPA) violation forfeitable as specified unlawful activity.
- Property involved in money laundering under 18 U.S.C. §1956, predicated on the IEEPA violation, as well as in wire and bank fraud.

³ Complaint, *United States v. All USD Tether Held in the Following Cryptocurrency Addresses*, No. 1:26-cv-08010 (S.D.N.Y. filed Sept. 14, 2026) [hereinafter Complaint].

- Assets of an entity engaged in a federal crime of terrorism (considering the material support to the IRGC, a designated foreign terrorist organization).

The Complaint alleges that between March 2024 and April 2024, Company-1 made 11 fund transfers totaling approximately \$37.15 million to Hexa Whale, and between November 2024 and March 2025, Company-1 made 32 funds transfers totaling approximately \$443.49 million to Blessed Trust. The Complaint describes that all of the transfers were processed through one or more correspondent accounts at a bank located in the SDNY.

As in prior stablecoin-forfeiture cases, the seizure warrant directs the stablecoin issuer to burn (*i.e.*, permanently destroy) the frozen tokens and issue new tokens of equal value into the FBI’s custody.⁴

Part of an Accelerating Pattern

This action sits at the convergence of several other recent, coordinated developments:

- **Increased focus on the digital assets sector.** On August 24, 2026, the Treasury Department launched “Operation Economic Outcast” in an effort to sever Iran’s remaining financial lifelines. Among other actions, Treasury’s Office of Foreign Assets Control (OFAC) issued a determination that Section 1(a)(i) of Executive Order 13902 applies to the digital assets sector of the Iranian economy. Under this authority, OFAC may impose sanctions on any person the secretary of the Treasury, in consultation with the secretary of State, determines to operate in the digital assets sector.⁵ OFAC used this new authority on September 17, 2026, to designate BitBank, an Iranian cryptocurrency exchange, and certain of its affiliated persons.⁶
- **Escalating designations of crypto infrastructure.** In April 2026, OFAC identified two wallets containing approximately \$344.2 million in USD stablecoin as property in which the Central Bank of Iran has an interest, and it added them to the SDN List. The stablecoin issuer subsequently froze the stablecoin in coordination with DOJ. Five weeks later, on June 2, 2026, OFAC went further, designating not just a single account, but four of Iran’s largest domestic cryptocurrency exchanges — Nobitex, Wallex, Bitpin and Ramzinex — together with four

⁴ Complaint ¶ 4, n. 1. This is by statutory design, as under the GENIUS Act, a permitted payment stablecoin issuer may operate lawfully only if it has the technical capability to “seize, freeze, burn, or prevent the transfer of” its tokens pursuant to a “lawful order,” and the GENIUS Act extends a comparable obligation to foreign issuers seeking U.S. market access through a digital asset service provider. Treasury’s proposed implementing rule goes further, requiring issuers to have real-time blocking and freezing capability across both primary and secondary market transactions.

⁵ Press Release, U.S. Dep’t of the Treasury, “[Treasury Launches Unprecedented Campaign Against Iranian Regime on Economic D-Day](#)” (Aug. 24, 2026); [Exec. Order No. 13902](#), 85 Fed. Reg. 2003 (Jan. 10, 2020).

⁶ OFAC, Press Release, “[Operation Economic Outcast Disrupts Digital Asset Exchange Enabling the Iranian Regime](#)” (Sept. 17, 2026).

SDNY's \$61 Million Crypto Forfeiture Action Reflects Growing Convergence of Civil Forfeiture and Sanctions Enforcement

of their executives. Treasury said the four exchanges together accounted for approximately 78% of Iran's total 2025 crypto volume, with Nobitex alone processing more than half of all Iranian digital asset inflows that year.⁷ The two actions represent an escalation, as OFAC targeted specific wallets tied to the Central Bank of Iran in April, then reached beyond individual wallets two months later to target the exchanges that carry most of the country's crypto volume.

- **Parallel civil forfeiture actions applying the same theory against other sanctioned jurisdictions.** In another recent action, DOJ sought civil forfeiture of more than \$7.74 million in stablecoins traced to North Korean IT-worker sanctions evasion.⁸ On September 3, 2026, Judge Rudolph Contreras of the U.S. District Court for the District of Columbia granted forfeiture of a portion of those funds under 18 U.S.C. § 981(a)(1)(C) as property traceable to IEEPA violations, while denying forfeiture of seven other wallet tranches for failure to satisfy Supplemental Rule G's notice-particularity requirement. The case demonstrates the same forfeiture theory DOJ is applying in the matter involving Blessed Trust and Hexa Whale and with respect to other Iran-linked parties is also successfully being applied in other contexts, and appears to be part of a coordinated strategy by DOJ and Treasury.⁹ (See our June 8, 2026, client alert "[North Korean Remote IT Worker Fraud: Managing Insider Threat, Sanctions and Employment Risk.](#)")
- **Judicial precedent lowering the evidentiary bar for tracing.** Multiple federal courts, including the U.S. Courts of Appeals for the First and Fifth Circuits, have held that customers of cryptocurrency exchanges have no such privacy expectation in records they voluntarily disclose to the exchange, analogizing them to bank records, which were at issue in the U.S. Supreme Court's seminal decision *United States v. Miller*, 425 U.S. 435 (1976).¹⁰ This line of authority is what makes the detailed blockchain-tracing in the SDNY complaint possible. Because exchange-held transaction records fall outside the Fourth Amendment's warrant requirement

under the third-party doctrine, the government can obtain them by subpoena or summons alone — no showing of probable cause is required. That access has enabled prosecutors to reconstruct the full flow of funds from Company-1 through Blessed Trust and Hexa Whale to the Entity A wallet addresses and onward to Nobitex and suspected IRGC fronts.

Together, these developments highlight how DOJ is pairing civil forfeiture's *in rem* theory and reduced burden of proof with Treasury's increased targeting of cryptocurrency exchanges and individual wallet addresses. The cooperation of wallet providers and digital asset issuers with such actions allows DOJ to reach non-U.S. actors whose contacts with the U.S. are otherwise minimal.

It is also worth noting that DOJ is deploying the same *in rem* mechanism beyond the sanctions context. For example, the U.S. Attorney's Office for the District of Columbia filed five civil forfeiture complaints in July 2026 seeking more than \$25 million in crypto traced to international investment- and romance-fraud schemes.¹¹ That action rests on a fraud predicate rather than IEEPA violations and illustrates that civil forfeiture is becoming a significant tool for DOJ to reach offshore crypto proceeds generally.

Practical Considerations

Robust know-your-customer (KYC) and customer due diligence processes, including sanctions screening, and effective transaction monitoring remain the best methods for financial institutions (such as cryptocurrency exchanges and virtual asset service providers (VASPs)) to identify potential sanctions-related touchpoints and other illicit financial activities.

In practical terms, that suggests several concrete steps:

- **Enhanced blockchain analytics.** Exchanges and VASPs should consider implementing on-chain monitoring tools capable of flagging wallets associated with sanctioned persons and other high-risk counterparties — including the kind of unhosted wallet clusters Entity A used to move funds to Nobitex and other IRGC-affiliated entities.
- **Strengthened KYC for high-risk counterparties.** Blessed Trust and Hexa Whale allegedly concealed their true business activities behind facially legitimate corporate descriptions. When engaging in high-risk activities or operating in higher-risk spaces like digital assets, financial institutions should consider whether and when to conduct enhanced due diligence on their customers and counterparties, such as by verifying

⁷ Press Release, U.S. Dep't of the Treasury, "[Economic Fury Targets Iran's Largest Digital Asset Exchange for Terror Finance and Sanctions Evasion](#)" (June 2, 2026); "[Three Enforcement Layers in Five Months: OFAC Designates Iran's Domestic Crypto Exchanges.](#)" TRM Labs (June 3, 2026).

⁸ *United States v. Virtual Currency Assoc. With North Korean IT Worker Money Laundering & Sanctions Evasion Conspiracies*, No. 25-cv-1769 (D.D.C. Sept. 3, 2026).

⁹ Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, "[Department Files Civil Forfeiture Complaint Against Over \\$7.74M Laundered on Behalf of the North Korean Government](#)" (June 5, 2025).

¹⁰ *Harper v. Werfel*, 118 F.4th 100, 107 (1st Cir. 2024) (holding that a Coinbase customer has no Fourth Amendment or property interest in exchange-held cryptocurrency transaction records under the third-party doctrine, and upholding an Internal Revenue Service (IRS) John Doe summons on that basis); *United States v. Gratkowski*, 964 F.3d 307, 310–11 (5th Cir. 2020) (holding that a person has no reasonable expectation of privacy in bitcoin records voluntarily held by a virtual currency exchange).

¹¹ Press Release, U.S. Att'y's Office, D.D.C., "[Investigations Into Cryptocurrency Scams Result in Seizure of More Than \\$25 Million](#)" (July 21, 2026).

SDNY's \$61 Million Crypto Forfeiture Action Reflects Growing Convergence of Civil Forfeiture and Sanctions Enforcement

beneficial ownership to a lower threshold (*e.g.*, 10% as opposed to 25%), identifying and verifying the customer's source of wealth and source of funds, and obtaining documentary evidence to substantiate the customer's stated business activities.

- **Proactive engagement with digital asset issuers' compliance programs.** The burn-and-reissue seizure method, while efficient, requires the cooperation of digital asset issuers. Exchanges and other financial intermediaries should understand the circumstances under which issuers will freeze tokens, whether in compliance with applicable law or at the request of

law enforcement, and factor that risk into their own custody and liquidity frameworks.

Final Thoughts

Given the recent pace of parallel Treasury and DOJ actions, we expect additional forfeiture filings applying the same or similar theories, as well as increased regulatory scrutiny of exchanges, digital asset issuers and trading intermediaries with exposure to sanctioned persons or jurisdictions.