FinCEN Whistleblower Bulletin:

Blow the Whistle on Iran-Related Illicit Finance

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) maintains a whistleblower incentive program for members of the public to submit information about violations of certain statutes enforced by Treasury and the Department of Justice (DOJ), including the Bank Secrecy Act (BSA) and the national security laws that serve as the foundation for the U.S. trade and economic sanctions administered by Treasury's Office of Foreign Assets Control (OFAC). By reporting information about suspected Iran-related violations of the BSA and economic sanctions, whistleblowers help strengthen our national security and keep America safe.

FinCEN welcomes tips from both U.S. and non-U.S. whistleblowers regarding individuals or entities that may be violating the BSA or OFAC-administered sanctions programs. This includes information about violations of these authorities that may involve the use of Iranian proxies and facilitators operating outside of Iran. Potential violations of OFAC sanctions require a nexus to the United States, including direct or indirect transactions with or involving the United States, U.S. persons, or entities owned or controlled by U.S. persons. Non-U.S. persons are also prohibited from certain dealings, including from causing U.S. persons to wittingly or unwittingly violate U.S. sanctions, conspiring to violate U.S. sanctions on Iran, and engaging in conduct that evades U.S. sanctions.

Operation Economic Outcast

Announced by Secretary Bessent on August 24, 2026, dubbed Economic D-Day, Operation Economic Outcast is severing the remaining economic lifelines that sustain the Iranian regime. Treasury has mapped the networks, facilitators, and financial channels that Iran uses to smuggle oil, evade sanctions, and fund terror. Working with partners across the U.S. government, the European Union, United Kingdom, Gulf partners, and others, Treasury is targeting any source of the regime's illicit revenue, as well as its sanctions evasion schemes to move funds.

Treasury warned that any entity facilitating money laundering or sanctions evasion on behalf of Iran risks being cut off from the U.S. financial system. It also expanded secondary sanctions exposure for those who continue doing business with the Iranian regime and will accelerate the pace of U.S. enforcement. More information on Operation Economic Outcast is available here.

What To Look For

Individuals potentially eligible for the whistleblower program may have direct knowledge of an individual or entity facilitating Iranian sanctions evasion or money laundering.

Iranian sanctions evasion may include one or more of the following typologies:

- Use of company types and jurisdictions at higher risk for Iranian sanctions evasion, including those from Iraq, the United Arab Emirates (UAE), Türkiye, and China
- Irregularities in shipping documentation that may hide links to Iran, including efforts to disguise the true identity of vessels used for shipments
- Payments to or from digital asset exchanges or service providers located in Iran or that may be front companies for such entities
- Shipping companies with Iranian counterparties, including those from Iraq, the UAE and China, especially Hong Kong
- Unusual use of exchange houses, including where the fees, number of transactions, or pattern of transactions do not reflect standard and customary commercial practices
- Unusual digital asset payments by petroleum, shipping, trading, or trust companies
- Unregistered peer-to-peer exchanges, foreign-located money services businesses, and nested digital asset exchanges.

Illicit finance schemes involving Iran's terrorist proxies may include:

- Transactions between customers include key terms known to be associated with terrorism or terrorist organizations, including in notes accompanying a peer-to-peer transfer
- Customer transactions with money services business (MSBs), including those involved in digital assets, or other financial institutions that operate in jurisdictions known for, or at high risk for, terrorist activity and are reasonably believed to have lax customer identification and verification processes, opaque ownership, or otherwise fail to comply with AML/CFT best practices
- Customer transactions that originate with, are directed to, or otherwise involve entities that are front companies, general "trading companies" with unclear business purposes, or other companies whose beneficial ownership information indicates that they may have a nexus with Iran or other Iran-supported terrorist groups
- Charitable organizations or non-profits that solicit donations but do not appear to provide any charitable services or openly supports terrorist activity or operations
- Customers that receive numerous small digital asset payments from many wallets, then transfers the funds to another wallet, particularly if the customers log in using an Internet Protocol (IP) based in a jurisdiction known for, or at high risk for, terrorist activity
- Money transfers by a customer to a jurisdiction known for, or at high risk for, terrorist activity that are inconsistent with the customer's stated occupation or business purpose with vague stated purposes such as "travel expenses," "charity," "aid," or "gifts"
- Accounts that have recently received large payouts from social media fundraisers or crowdfunding platforms that are accessed using an IP address in a jurisdiction known for, or at high risk for, terrorist activity where the account holder is not known to reside or have traveled.

For additional information on Iranian sanctions evasion and illicit finance schemes, OFAC and FinCEN regularly publish guidance.

- OFAC has issued alerts on Sanctions Risks of Iranian Demands for Strait of Hormuz Passage and Sanctions Risk of Dealing with Teapot Oil Refineries, as well as Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion. Information and advisories about OFAC's Iran sanctions may be found here.
- FinCEN has issued three recent advisories on Iranian Procurement Efforts for its Commercial Aviation Industry; Oil Smuggling, Shadow Banking, and Weapons Procurement by the Iranian regime; and Front Companies, Financial Facilitators, and Digital Assets Infrastructure connected to Iran's Islamic Revolutionary Guard Corps. FinCEN has also issued a Financial Trend Analysis that includes case studies of Iran's use of shadow banking networks of exchange houses and foreign companies to evade sanctions.

How to Blow the Whistle

Individuals who voluntarily provide information about violations or conspiracies to commit violations of covered statutes[1] may be eligible for awards if the information they provide leads to a successful enforcement action by Treasury or DOJ that results in the collection of monetary penalties exceeding $1,000,000, and the requirements in 31 U.S.C. 5323 and its implementing regulation are otherwise met. Awards offered under FinCEN's whistleblower program can be substantial—10 to 30 percent of collected monetary penalties—and are designed to encourage individuals with visibility into such violations of law to provide Treasury with high quality and actionable information. At Treasury's discretion, awards may be paid to individuals who, directly or indirectly, work for or on behalf of the Iranian regime or Iranian state-owned enterprises if all other relevant program requirements are met.

To learn more about FinCEN's whistleblower program, including how to submit a tip, visit FinCEN's webpage for the Office of the Whistleblower.

1 *See* 31 U.S.C. 5323. The statutes covered by FinCEN's whistleblower program are subchapter II of chapter 53 of title 31, United States Code; chapter 35 or section 4305 or 4312 of title 50, United States Code; and the Foreign Narcotics Kingpin Designation Act (21 U.S.C. 1901 *et seq.*).