FinCEN ALERT

FIN-2026-Alert002 **May 11, 2026**

FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "**FIN-2026-Alert002**."

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to assist financial institutions[1] in identifying actors suspected of funding and facilitating procurement networks supporting the Islamic Revolutionary Guard Corps (IRGC) and mitigating those risks through the filing of suspicious activity reports (SARs).[2] The IRGC was created after the Iranian Revolution as a parallel organization to Iran's regular armed forces that reports directly to Iran's Supreme Leader and is charged with defending the Iranian regime. The IRGC includes ground, naval, and air forces, along with the Basij internal security militia, and the IRGC-Qods Force (IRGC-QF). The IRGC-QF conducts covert operations abroad and supports terrorism by supplying funding, training, and weapons to aligned groups.[3] Since its inception, the IRGC has engaged in terrorist activity with the support of the Iranian government and is a designated Foreign Terrorist Organization (FTO).[4]

As described in FinCEN's 2025 Iran Advisory, the IRGC relies on complex financial facilitation networks comprised of exchange houses, front companies, financial facilitators, and other service providers operating across multiple jurisdictions to obscure beneficial ownership, disguise the origin of funds, and enable movement of proceeds linked to sanctions evasion and other illicit activity.[5] In addition, recent analysis of Bank Secrecy Act (BSA) data indicates that the IRGC relies on networks of shell companies and financial facilitators to launder digital asset proceeds through

1. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
2. For more information about the IRGC, see Director of National Intelligence (DNI) National Counter Terrorism Center (NCTC), "Islamic Revolutionary Guard Corps (IRGC)" ("Mar. 2025 NCTC IRGC") (Mar. 2025).
3. *See* Mar. 2025 NCTC IRGC, *supra* note 2; Congressional Research Service (CRS), "Iran: Background and U.S. Policy" (updated May 22, 2025), at p. 4.
4. The IRGC, including the IRGC-QF, was designated as an FTO in April 2019. *See* Department of State, "Designation of the Islamic Revolutionary Guard Corps" (Apr. 8, 2019).
5. *See* FinCEN, FIN-2025-A002, "FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts" ("June 2025 FinCEN Iran Advisory") (June 6, 2025).

layered corporate structures and cross-border transactions. These entities function as instruments of the IRGC by moving funds, converting assets, or otherwise acting on behalf of sanctioned actors, even where the companies themselves are not formally identified as IRGC-owned. This structure allows the IRGC and its affiliates to access the financial system and disguise control while avoiding direct attribution.

This Alert reminds financial institutions of their BSA reporting obligations and encourages vigilance against sanctions evasion, terrorist financing, and other illicit activity that may be connected with the IRGC. On February 4, 2025, President Trump signed National Security Presidential Memorandum-2 (NPSM-2), imposing a policy of maximum pressure on the Iranian regime and driving a whole-of-government approach to deny Iran all paths to a nuclear weapon and counter its malign influence.[6] Iran as well as the IRGC are subject to comprehensive U.S. sanctions,[7] including a prohibition on opening or maintaining correspondent accounts in the United States for, or on behalf of, Iranian financial institutions pursuant to Section 311 of the USA PATRIOT Act pursuant to a finding that the jurisdiction of Iran is a primary money laundering concern.[8] Furthermore, FinCEN notes that the Financial Action Task Force (FATF) has long identified Iran as a high-risk jurisdiction, and recently re-iterated the need for countries to apply effective countermeasures,[9] including calling on all jurisdictions to prohibit Iranian digital asset service providers from establishing or maintaining a presence in their countries or establishing relationships with their digital asset service providers, along with limiting digital asset transactions with Iran.[10]

The information contained in this Alert is derived from FinCEN's analysis of BSA data, open-source reporting, and law enforcement information. This Alert supplements the information related to Iranian illicit finance outlined in FinCEN's 2025 FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts and FinCEN's 2024 Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations.[11] FinCEN welcomes any feedback from financial institutions on this Alert, its utility, or other best practices or control limitations in addressing the typologies or red flag indicators described herein. Please submit feedback to FinCEN at www.fincen.gov/contact.

6. *See* White House, "National Security Presidential Memorandum-2" (Feb. 4, 2025).
7. The U.S. maintains comprehensive sanctions on Iran, which prohibit most transactions and activities with Iran by U.S. persons or within the United States, unless exempt or authorized by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). Under U.S. sanctions, U.S. persons are generally prohibited from engaging in transactions with Iran's Islamic Revolutionary Guard Corps, which is sanctioned pursuant to several authorities, including nonproliferation and counterterrorism sanctions, and is a designated Foreign Terrorist Organization. For more information, see OFAC, "Iran Sanctions," (accessed Apr. 30, 2026).
8. The final rule imposing a special measure against Iran as a jurisdiction of primary laundering concern defines "covered financial institution" with the same definition used in the final rule implementing the provisions of Section 312 of the USA PATRIOT Act. *See* FinCEN, "Imposition of Fifth Special Measure Against the Islamic Republic of Iran as a Jurisdiction of Primary Money Laundering Concern," 84 FR 59302 (Nov. 14, 2019); 31 C.F.R. § 1010.661.
9. *See* Treasury, "Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering, Combating the Financing of Terrorism, and Counter-Proliferation Finance Deficiencies" (Mar. 6, 2026).
10. *See* FATF, "High-Risk Jurisdictions subject to a Call for Action" (Feb. 13, 2026).
11. *See* June 2025 FinCEN Iran Advisory, *supra* note 5; FinCEN, FIN-2024-A001, "FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations" ("May 2024 FinCEN Advisory") (May 8, 2024).

Commodity Sales and Misrepresentation of Commercial Activity

The IRGC and its subordinate units supplement their budgets by smuggling oil to international buyers, the proceeds of which fund procurement, domestic weapons development, and terrorist activity abroad.[12] In its 2025 Financial Trend Analysis (FTA) on Iranian Shadow Banking, FinCEN found that oil companies potentially linked to Iran transacted approximately $4 billion in 2024.[13] The FTA also found that dozens of shipping companies—mostly based in Iraq, the United Arab Emirates (UAE), and Hong Kong—potentially related to the transport of sanctioned Iranian oil and petrochemicals conducted transactions through U.S. correspondent accounts totaling approximately $707 million over the same period.[14]

To transport the oil, the IRGC and other Iranian actors use a fleet of old and poorly maintained vessels that operate outside of standard maritime regulations, sometimes referred to as the "shadow fleet," "ghost fleet," or "dark fleet." These vessels are often owned, managed, or leased by shipping or front companies outside of Iran,[15] and they engage in deceptive shipping practices to hide the intended destination of their cargo.[16] To further disguise its origins, Iranian oil is sometimes blended with oil from third countries or relabeled with forged documents as the product of another jurisdiction, most commonly as "Malaysian blend."[17] The overwhelming majority of this oil is sold to small independent oil refineries in China, sometimes called "teapot refineries."[18]

Use of Front Companies and Layered Corporate Structures

The IRGC and other Iranian actors rely on multi-jurisdictional "shadow banking" networks comprised of exchange houses, trading companies, and front companies to sell oil and other commodities abroad, launder the proceeds, and then procure weapons and other materiel on the international market. Various Iranian banks have established "rahbar" companies to manage their clients' international transactions.[19] These companies use Iranian exchange houses to establish front companies in third-country jurisdictions to obscure Iranian involvement and layer

12. *See* May 2024 FinCEN Advisory, *supra* note 11, at pp. 2–3.
13. FinCEN, Financial Trend Analysis, "FinCEN Financial Trend Analysis, Iranian Shadow Banking: Trends in Bank Secrecy Act Data October 2025" ("Oct. 2025 FinCEN Iran FTA") (Oct. 23, 2025), at p. 6.
14. *Id.*, at p. 10.
15. *See* June 2025 FinCEN Iran Advisory, *supra* note 5, at p. 4.
16. For more information about deceptive shipping practices, see generally OFAC, "Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion" (Apr. 16, 2025) and Treasury, "Treasury Takes Massive Action Against High-Profile Iranian Network" ("July 2025 Treasury Press Release") (July 30, 2025).
17. *See* June 2025 FinCEN Iran Advisory, *supra* note 5, at p. 4; *see also* Treasury, "Treasury Sanctions Networks Enabling Illicit Trade that Benefits IRGC-QF and Hizballah" (Sept. 25, 2024); "Treasury Targets Diverse Networks Facilitating Iranian Oil Trade" (July 3, 2025); "Treasury Tightens Sanctions on Iran's Oil Network Supporting its Military" ("Nov. 2025 Treasury Press Release") (Nov. 20, 2025).
18. *See* June 2025 FinCEN Iran Advisory, *supra* note 5, at p. 3.
19. *See* Treasury, "Secretary Bessent Announces Sanctions Against Architects of Iran's Brutal Crackdown on Peaceful Protests" (Jan. 15, 2026).

transactions, often exploiting permissive jurisdictions and free trade zones that offer favorable conditions for company formation.[20] These front companies are then used to establish bank accounts outside of Iran that enable sanctioned entities to access the international banking system to transact with foreign entities. By using front company accounts outside Iran to receive and remit payments, sanctioned entities like the IRGC are able to conduct transactions through the international financial system without repatriating funds to Iran.[21] In its 2025 FTA, FinCEN found likely shell companies, matching indicators for shell and Iranian activity, moved $5 billion in 2024, primarily from non-resident accounts at banks in China operated by Hong Kong-based companies to the UAE.[22]

U.S. financial institutions may indirectly detect Iran-linked rahbar companies and exchange houses when processing U.S. dollar-denominated payments for foreign correspondents. Indicators include recently incorporated entities transacting in unusually large sums, rapid movement of funds, transactions between companies in disparate lines of business, and large, round dollar payments. Treasury also continues to encourage U.S. financial institutions to exercise heightened vigilance with respect to certain correspondent relationships and to carefully consider whether it may be appropriate to require certain respondents to apply strengthened controls, such as targeted monitoring, heightened due diligence, or additional training.

Use of Facilitators and Other Service Providers

IRGC oil smuggling and shadow banking networks are bolstered by a vast web of facilitators, including money services businesses (MSBs), investment companies,[23] and trust and company service providers, which assist—wittingly and unwittingly—in orchestrating complex money laundering and sanctions evasion schemes.[24] According to FinCEN analysis, purported trust companies and affiliates—including those based in Hong Kong and Eastern Europe—have been identified as facilitating the transmission of value to the IRGC, including through the conversion of fiat currency to digital assets, particularly the minting of stablecoins.

To bring its oil to market, for example, the IRGC relies on brokers operating in third-country jurisdictions and a multi-jurisdictional network of logistics and shipping facilitators. These facilitators provide maritime support services, such as bunkering, supplies, insurance, and short-term financing, which Iranian regime-affiliated actors usually pay for using front companies

20. *See* Oct. 2025 FinCEN Iran FTA, *supra* note 13, at pp. 14–17.

21. *See* June 2025 FinCEN Iran Advisory, *supra* note 5, at pp. 3, 5.

22. These indicators included recent incorporation with limited or no internet presence; large transactions with an unclear business purpose; and companies that shared addresses, financial activity, counterparties, and name similarities with OFAC-designated Iranian companies. *See* Oct. 2025 FinCEN Iran FTA, *supra* note 13, at p. 8.

23. FinCEN's 2025 Iran FTA found that a small cadre of investment companies closely linked with Iran-linked oil companies appear to provide Iranian entities—either wittingly or unwittingly—with access to foreign investment trading markets, potentially including foreign commodities futures markets. For more information, see Oct. 2025 FinCEN Iran FTA, *supra* note 13, at p. 11.

24. *See* June 2025 FinCEN Iran Advisory, *supra* note 5, at p. 5.

operating outside Iran.[25] These facilitators often provide services to multiple illicit actors. For example, Iranian facilitator Mohammad Hossein Shamkhani, who was designated by Treasury's Office of Foreign Assets Control (OFAC) in July 2025, uses his network's vast fleet of vessels, ship management firms, and front companies—some of which pose as legitimate financial services firms—to launder billions in profits from both Iranian and Russian crude oil and other petroleum products.[26]

In addition, the IRGC often engages in oil smuggling and launders the proceeds in conjunction with terrorist partner and proxy groups such as Ansarallah[27] and Lebanese Hizballah (Hizballah), which have their own global networks of facilitators and intermediaries.[28] Hizballah, for example, launders funds through networks of businesses in West Africa, Europe, and South America. Hizballah also leverages a broad network of intermediaries, such as Lebanon-based trusts and non-governmental organizations; unlicensed MSBs, some of which it controls; and informal value transfer systems like the Hawala system.[29]

Use of Digital Assets

According to industry reporting, the volume of Iranian digital assets activity has reached billions of dollars per year. Iranian government entities, including the IRGC, conduct sanctions evasion as part of this activity.[30] In addition, according to press reporting, Iran has stated its intent to use digital assets to collect illegal payments from oil tankers attempting to freely navigate passage through the Strait of Hormuz.[31] Iranian proxies such as Hamas and Hizballah have also used digital assets to raise, launder, and transfer funds. For example, Hamas has sought digital asset contributions in donation drives since at least 2019 and has historically leveraged digital asset service providers (DASPs) in an attempt to safeguard the anonymity of its donors.[32] Iranian government-affiliated cyber actors also use digital assets in support of their malicious cyber activity, such as ransomware campaigns targeting U.S. organizations.[33]

25. *Id*., at pp. 3–4.
26. *See* July 2025 Treasury Press Release, *supra* note 16; *see also* Nov. 2025 Treasury Press Release, *supra* note 17.
27. Ansarallah, commonly referred to as the Houthis, is a designated FTO. *See* State, "Designation of Ansarallah as a Foreign Terrorist Organization" (Mar. 4, 2025).
28. *See* Treasury, "Treasury Targets Qods Force, Houthi, and Hizballah Finance and Trade Facilitators" (Mar. 26, 2024); Treasury, "Treasury Adds Further Sanctions Targeting Houthi and Hizballah Trade Networks" (Aug. 15, 2024).
29. *See* FinCEN, FIN-2024-Alert003, "FinCEN Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities" (Oct. 23, 2024), at pp. 5–6.
30. *See* Chainalysis, "Inside Iran's Growing $7.8 Billion Crypto Ecosystem: IRGC Dominance and a Flight to Bitcoin Reflect Geopolitical Tensions and Domestic Unrest" (Jan. 15, 2026) (accessed Apr. 13, 2026); Elliptic, "The Central Bank of Iran has acquired US dollar stablecoins worth at least half a billion dollars" (Jan. 21, 2026) (accessed Apr. 13, 2026); TRM Labs, "New Drones, Old Tactics: How Iran is Experimenting with Crypto to Fund Conflict and Evade Sanctions" (May 28, 2025) (accessed Apr. 13, 2026); TRM Labs, "Iran's Crypto Economy" (Apr. 16, 2023) (accessed Apr. 13, 2026).
31. Financial Times, "Iran demands crypto fees for ships passing Hormuz during ceasefire" (Apr. 8, 2026) (accessed Apr. 8, 2026); Wall Street Journal, "Iran's $7.8 Billion Crypto Economy Finds New Way to Grow After Cease-Fire" (Apr. 9, 2026) (accessed Apr. 13, 2026).
32. *See* FinCEN, FIN-2024-A001, "FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations" (May 8, 2024), at pp. 7, 10.
33. *See* Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Department of Defense

Digital asset transactions serve as one leg of Iran's shadow banking network, functioning as part of a complex transactional structure designed to obfuscate Iranian involvement. Because digital assets can be quickly transferred internationally without intermediary financial institutions, digital assets enable Iranian facilitators to circumvent the traditional financial system. Like other illicit actors, Iranian facilitators are likely to use stablecoins for this purpose, due to stablecoins' relative liquidity, ease of settlement, and exchange rate stability.[34] Iran is also adapting its abuse of stablecoins in its continued efforts to evade sanctions. According to FinCEN analysis, Iran's use of stablecoins includes minting[35] and moving between large volume stablecoin issuers as well as the creation of proprietary stablecoins, such as USDZ, the stablecoin associated with OFAC-designated stablecoin issuer Zedxion.[36]

Iranian actors use of a variety of mechanisms to access digital assets. Iran-based DASPs play a role in enabling Iranian digital assets activity and connectivity with the global digital assets ecosystem.[37] Consequently, U.S. financial institutions with exposure to digital assets should consider reviewing blockchain ledgers for activity attributed to Iran-based DASPs, including indirect connections to such activity. Institutions should also be aware that the international digital assets industry is highly dynamic; new digital assets businesses may incorporate or operate in Iran with little notice or footprint, making it especially important to assess the risks of recently established digital asset businesses. Further, unregistered peer-to-peer (P2P) exchangers[38] and unregistered foreign-located MSBs[39] may offer digital asset-related services in Iran. Financial institutions should be aware that these unregistered digital asset exchangers typically rely on the liquidity provided by larger DASPs to process transactions.[40]

Cyber Crime Center, "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations" (Aug. 28, 2024).

34. Stablecoins are a type of digital asset for which the value of the token is tied to another asset, typically a fiat currency such as the U.S. dollar. *See* Treasury, "2026 National Proliferation Financing Risk Assessment" (Mar. 2026), at p. 16; *see also* Treasury, "2026 National Money Laundering Risk Assessment" ("2026 NMLRA") (Mar. 2026), at pp. 52–53.

35. Minting is the process through stablecoin issuers create new stablecoin tokens. *See* Watsky, Cy, Jeffrey Allen, Hamzah Daud, Jochen Demuth, Daniel Little, Megan Rodden, and Amber Seira, "Primary and Secondary Markets for Stablecoins," FEDS Notes (2024), Washington: Board of Governors of the Federal Reserve System, (Feb. 23, 2024).

36. *See* Treasury, "Treasury Sanctions Iranian Regime Officials for Violent Repression and Corruption" ("Jan. 2026 Treasury Press Release") (Jan. 30, 2026).

37. For industry analysis illustrating how Iranian DASPs may interact with the broader digital assets ecosystem, *see*, *e.g.*, TRM Labs, "Iran's Crypto Economy" (Apr. 16, 2023); Elliptic, "The Central Bank of Iran has acquired US dollar stablecoins worth at least half a billion dollars" (Jan. 21, 2026); Chainalysis, "OFAC Targets $600 Million Iranian Shadow Banking Network Using Cryptocurrency to Evade Sanctions" (Sept. 16, 2025).

38. P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements, online forums, social media, and through word of mouth. *See* FinCEN, FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" ("FinCEN CVC Advisory") (May 9, 2019), at pp. 4–5.

39. Foreign-located MSBs that do not adhere to AML/CFT requirements and standards are popular among illicit users of digital assets seeking to move funds in and out of the United States and represent a significant money laundering vulnerability. *See* FinCEN CVC Advisory, *supra* note 38, at p. 6.

40. DASPs that offer trading services and pool customer deposits into an account hosted by a larger exchange are referred to as "nested exchanges." Nested exchanges may operate fully or partially within the infrastructure of the host provider, rather than as a unique entity, potentially providing illicit actors with an additional layer of obfuscation. *See*

Uneven and often inadequate regulation and supervision of digital assets—including a lack of implementation of FATF standards—across jurisdictions also enables Iranian facilitators to access digital assets through international DASPs.[41] In the past, Iranian actors have accessed digital assets by exploiting gaps in DASPs' anti-money laundering and countering the financing of terrorism (AML/CFT) and sanctions compliance programs. For example, DASPs have overlooked indicators connecting accounts or transactions to Iran, such as references to Iran in onboarding documents, invoices, or other documentation, or customer accounts accessed from Iranian Internet Protocol (IP) addresses.[42] More recently, Iranian actors utilizing digital assets have turned to more sophisticated methods, such as the creation of DASP front companies. For example, Zedcex Exchange, Ltd. and Zedxion Exchange, Ltd., which were designated by OFAC in January 2026, are two United Kingdom-registered digital asset exchanges with connections to an Iranian businessman and sanctions evader. Multiple digital asset addresses attributed to those exchanges processed funds for wallets linked to the IRGC.[43]

Case Study: Treasury Targets Financial Network Supporting Iran's Military[44]

In September 2025, OFAC designated a pair of Iranian financial facilitators and more than a dozen Hong Kong- and UAE-based individuals and entities for their roles in coordinating funds transfers, including from the sale of Iranian oil, that benefited the IRGC-QF and Iranian Ministry of Defense and Armed Forces Logistics (MODAFL).

Between 2023 and 2025, Iranian nationals Alireza Derakhshan (Derakhshan) and Arash Estaki Alivand (Alivand) facilitated the purchase of over $100 million in digital assets for oil sales to benefit the Iranian government. Derakhshan and Alivand used a network of front companies in multiple foreign jurisdictions to transfer the digital assets.

Alivand worked as a financial facilitator and oil broker for the Syria-based Al-Qatirji Company, which served as a primary partner of the IRGC-QF in the sale of Iranian oil. In 2023, Alivand coordinated a payment from Minato Commercial Brokers, a front company utilized by Derakhshan, to an Al-Qatirji Company account. Alivand was also involved in transactions worth millions of dollars with a Hizballah-associated money changer who provided Hizballah with access to digital wallets to receive funds related to IRGC-QF commodity sales, and who conducted digital asset transfers on behalf of the previously designated Al-Qatirji Company.

2026 NMLRA, *supra* note 34, at p. 51.

41. *See* 2026 NMLRA, *supra* note 34, at pp. 49–50.

42. *See, e.g.*, Treasury, "Exodus Movement, Inc. Settles with OFAC for $3,103,360 for Apparent Violations of Iran-related Sanctions Regulations" (Dec. 16, 2025); Treasury, "OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Programs" (Nov. 21, 2023); Treasury, "OFAC Settles with Virtual Currency Exchange Kraken for $362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations" (Nov. 28, 2022); Treasury, "OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions" (Feb. 18, 2021).

43. *See* Jan. 2026 Treasury Press Release, *supra* note 36.

44. Treasury, "Treasury Targets Financial Network Supporting Iran's Military" (Sept. 16, 2025).

Red Flag Indicators for Iranian Sanctions Evasion Activity

FinCEN has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to Iranian sanctions evasion and other illicit activities. These red flags supplement the red flags identified in FinCEN's 2025 Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts, all of which remain relevant.[45] As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the totality of available facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags before determining that a behavior or transaction is suspicious.

Oil Smuggling-Related Red Flags

1. **Shipping Companies with Iranian Counterparties.** Transactions involving a petroleum or shipping company reveal that it does business with counterparties that have ties to Iran or transport goods using "shadow fleet" vessels that have ties to Iran or that maritime databases indicate have made stops at Iranian ports.
    - *Financial institutions may consider ensuring their correspondent account holders conduct due diligence on their customers for prior connections to Iran or Iranian counterparties.*

2. **Irregularities in Shipping Documentation that may be Intended to Hide Activities Involving Iran.** A customer makes oil-related transactions and wire transfers involving vessels that have been previously linked to suspicious financial activities or that include documentation, such as bills of lading or shipping invoices, with no consignees, that appear to be falsified, or that omit key information, to obfuscate the Iranian nexus.
    - *Financial institutions may consider requiring a review of shipping documentation to identify falsified or missing information where practical.*

3. **Efforts to Disguise Vessel Information and Ownership.** Documentation associated with a customer's oil-related transactions references vessels that, according to maritime databases, have undergone recent or multiple name or flag changes, or transfer of ownership or operation to another person following OFAC's designation of its owner or operator, but the designated owner or operator appears to maintain an interest in the vessel.
    - *Financial institutions may consider requiring due diligence on vessels to determine whether they have undergone recent name, flag, or ownership changes, including transfer from sanctioned persons.*

45. *See* June 2025 FinCEN Iran Advisory, *supra* note 5, at pp. 8–9.

4 **Efforts to Disguise Oil Origins.** Documentation associated with a customer's oil-related transactions references "Malaysian blend" oil, particularly if the vessel is bound for China by way of Southeast Asia and if maritime databases indicate that the vessel displayed Automatic Information System (AIS) irregularities during its voyage or reveal evidence of a ship-to-ship transfer in geographic areas of concern or without commercial need.

- *Financial institutions may consider requiring heightened due diligence on any transactions referencing "Malaysian blend" oil, particularly if the transactions show other indications of oil smuggling.*

Shadow Banking and Front Company Abuse-Related Red Flags

5 **Unclear Sources of Funds.** A customer receives wire transfers or deposits that do not contain any information about the source of funds, contain incomplete information about the source of funds, or do not match the customer's line of business, and they involve entities in a high-risk jurisdiction for Iranian illicit finance-related activity.

- *Financial institutions may consider reviewing relationships with clients that show a pattern of opaque business dealings in jurisdictions at high risk for IRGC abuse.*

6 **Use of Company Types and Jurisdictions at High-Risk for IRGC Abuse.** A general trading company with opaque ownership registered in a commercial free trade zone in the UAE or other location and whose trading counterparties are companies mostly located in jurisdictions such as Singapore and Hong Kong has bank accounts at multiple financial institutions in locations such as China, Hong Kong, Oman, or the UAE.

- *Financial institutions may consider conducting heightened due diligence on company types that are at high risk for IRGC abuse.*

7 **Likely Front Companies that Exhibit Transaction Patterns Typical of IRGC Shadow Banking.** A company registered in Hong Kong that banks using a Chinese non-resident account has little to no web presence, is co-located with numerous other similar companies, or is recently incorporated yet transmitting large, round dollar payments with no adequate explanation for the source of funds, or makes numerous payments in large figures to UAE general trading companies or commercial free trade zone-based intermediaries with no clear business purpose.

- *Financial institutions should consider conducting heightened due diligence on recently formed companies transacting in unusually high amounts that exhibit payment patterns typical of Iranian shadow banking.*

8 **Unusual Use of Exchange Houses.** A customer makes transactions that move through multiple exchange houses and/or trading companies, adding additional fees and costs as the transactions progress, where the fees, number of transactions, or pattern of transactions do not reflect standard and customary commercial practices.

- *Financial institutions may consider conducting heightened due diligence on customers that make frequent or unusual use of exchange houses in jurisdictions at high risk for IRGC activity.*

Digital Assets-Related Red Flags

9 **Unusual Digital Asset Payments by Petroleum, Shipping, Trading, or Trust Companies.** A company engaged in a line of business with potential exposure to Iranian oil smuggling deviates from normal business practices to send or receive payments using digital assets.

- *Financial institutions may consider conducting heightened due diligence for companies using digital assets to effect significant payments in cases where the underlying transaction could be related to Iranian oil.*

10 **Stablecoin Payments with an Unclear Source of Funds.** A customer in a high-risk jurisdiction for Iranian illicit finance-related activities receives a stablecoin payment that does not match the customer's line of business and fails to provide information about the source of funds or provides documentation indicating a potential link to Iranian illicit finance.

- *Financial institutions may consider requesting documentation from customers regarding the source of digital asset payments that involve entities in a high-risk jurisdiction for Iranian illicit finance-related activity.*

11 **Unusual Stablecoin Account Activity.** A customer of a stablecoin issuer, particularly a foreign entity such as an overseas purported trust company, opens an account and subsequently engages in mint activity requiring multiple rate/limit increases in a short period of time, or otherwise transacts in a manner that does not appear consistent with its reported business profile.

- *Financial institutions may consider requesting documentation from customers regarding the source of stablecoin payments that involve entities in a high-risk jurisdiction for Iranian illicit finance-related activity.*

12 **Payments to or from an Iran-located DASP.** Blockchain analysis indicates that a customer account transacted directly or indirectly with a digital asset address attributed to an Iranian entity.

- *Financial institutions may consider using blockchain analytics to identify digital asset transactions that may be connected to a known Iranian entity.*

13 **Iran-related Cyber Indicators.** Authentication and account activity indicates that a user may be conducting digital asset transactions from Iran. For example, activity logs may show connections from Iranian IP addresses, or sharing IP addresses or common devices with users previously identified as having an Iranian nexus, authentication using an Iranian email service or Iranian telephone number, or use of a device with time zone, language, and other settings consistent with a location in Iran. Connection through a virtual private network (VPN), residential proxy network, or Tor exit node—when combined with other evidence of a location in Iran—may indicate an attempt by an Iranian user to circumvent geofencing. In reporting such activity, financial institutions may also be able to provide associated technical details such as IP addresses with time stamps, device identifiers, and indicators of compromise that can provide helpful information to authorities.[46]

46. *See* FinCEN, "Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs)" (Oct. 25, 2016).

- *Financial institutions may consider screening cyber indicators such as IP addresses for evidence that an account has been accessed from Iran or by an Iranian entity.*

14 **Unregistered P2P Exchangers, Foreign-Located MSBs, and Nested DASPs.** Account activity indicates that a customer may operate as an unregistered P2P exchanger, foreign-located MSB, or nested DASP that provides services in Iran. For example, a customer of a DASP who is located in a high-risk jurisdiction for Iranian illicit finance-related activity appears to be using liquidity provided by the DASP to execute large numbers of offsetting transactions.

- *Financial institutions may consider heightened monitoring of customer accounts for activity associated with potential operation of an unregistered P2P exchanger, foreign-located MSB, or nested DASP for customers with possible exposure to Iranian counterparts.*

FinCEN requests that financial institutions reference this Alert by including the key term **"FIN-2026-Alert002"** in SAR field 2 (Filing Institutions Note to FinCEN) and the narrative, and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization).

Financial institutions wanting to expedite their report of suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[47]

For Further Information

FinCEN's website, at www.fincen.gov, contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Alert should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

47. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.