



FinCEN ADVISORY

FIN-2024-A001

May 08, 2024

FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations

In light of intensified terrorist activity in the Middle East, FinCEN urges vigilance in identifying potential suspicious activity related to the financing of Iran-backed militias and terrorist organizations, including Hamas, the Houthis, Hizballah, Palestinian Islamic Jihad (PIJ), and Iran-aligned militia groups in Iraq and Syria.

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this advisory in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "**IRANTF-2024-A001**" and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization).

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist financial institutions in detecting potentially illicit transactions related to Islamic Republic of Iran (Iran)-backed terrorist organizations amid intensified terrorist activity in the Middle East.¹ Recent events have underscored Iran's involvement in and financing of terrorist activity in the region. Iran seeks, among other goals, to project power by exporting terrorism throughout the Middle East and beyond through the financing of a range of regional armed groups, some of which are U.S.-designated Foreign Terrorist Organizations (FTOs) or Specially Designated Global Terrorist

organizations (SDGTs).² These terrorist organizations include Lebanese Hizballah (Hizballah),³ Hamas,⁴

1. In 2018, FinCEN published an advisory on Iran's exploitation of the international financial system, which continues to serve as an additional resource for financial institutions in identifying suspicious activity related to Iran. See FinCEN, "[Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System](#)" ("Oct. 2018 FinCEN Advisory") (Oct. 11, 2018). While the Oct. 2018 FinCEN Advisory and this advisory address U.S. sanctions that prohibit U.S. persons and U.S.-owned or -controlled foreign entities from engaging in transactions involving Iran, including persons "ordinarily resident" in Iran, financial institutions should note that some transactions involving Iran, Iranian citizens, or persons with connections to Iran, including certain humanitarian transactions, may be authorized by general or specific license or exempt from sanctions prohibitions. Institutions should regard an Iranian nexus and the typologies listed in this advisory as factors to consider when assessing whether any specific transaction or activity has an illicit nexus or is otherwise prohibited.
2. Congressional Research Service (CRS), "[Iran: Background and U.S. Policy](#)" ("Jan. 2024 CRS Report") (Jan. 26, 2024), at pp. 2-4.
3. Lebanese Hizballah was designated as an FTO on October 8, 1997, by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended, and as an SDGT by the Secretary of the Treasury pursuant to Executive Order (EO) 13224 on October 31, 2001. For more information about Lebanese Hizballah, see Directorate of National Intelligence's (DNI) National Counterterrorism Center (NCTC), "[Counter Terrorism Guide: Lebanese Hizballah](#)" (Sept. 2022).
4. Hamas was designated as an FTO on October 8, 1997, by the Secretary of State in accordance with section 219 of the INA, as amended, and as an SDGT by Treasury pursuant to EO 13224 on October 31, 2001. For more information about Hamas, see DNI's NCTC, "[Counter Terrorism Guide: HAMAS](#)" (Sept. 2022).

the Palestinian Islamic Jihad (PIJ),⁵ the Houthis (Ansarallah),⁶ and several Iran-aligned militia groups in Iraq and Syria. As demonstrated by the October 7, 2023, Hamas attack on Israel and recent Houthi attacks in the Red Sea,⁷ these organizations are capable of perpetrating horrific violence, causing destruction, and disrupting critical supply chains. The U.S. Department of the Treasury (Treasury) has been systematically working to dismantle these organizations by disrupting their illicit finance networks and eliminating their sources of revenue.⁸

This advisory highlights the means by which terrorist organizations receive support from Iran and describes several typologies these terrorist organizations use to illicitly access or circumvent the international financial system to raise, move, and spend funds. It also provides red flags that may assist financial institutions in identifying related suspicious activity and is consistent with FinCEN's National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Priorities, which include terrorist financing.⁹

The information contained in this advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open-source reporting, and information provided by law enforcement partners.

How Iran Raises and Moves Funds in Support of Terrorism

Iran supports its numerous terrorist partners and proxies through the Islamic Revolutionary Guard Corps (IRGC), a parallel organization to Iran's regular armed forces.¹⁰ In particular, the IRGC division known as the IRGC-Qods Force (IRGC-QF)¹¹ is responsible for conducting covert lethal activities outside of Iran, such as supporting terrorism globally and serving as a conduit for funds, training, and weapons to Iran-aligned partners and proxies.¹²

5. PIJ was designated as an FTO on October 8, 1997, by the Secretary of State in accordance with section 219 of the INA, as amended. For more information about PIJ, see DNI's NCTC, "[Counter Terrorism Guide: Palestinian Islamic Jihad \(PIJ\)](#)" ("Feb. 2023 Counter Terrorism Guide") (Feb. 2023).
6. The Houthis were designated as an SDGT by the Department of State pursuant to EO 13224 on January 17, 2024, effective February 16, 2024. See Department of State, "[Terrorist Designation of the Houthis](#)" ("Jan. 2024 Houthi Designation") (Jan. 17, 2024).
7. See Deputy Secretary of the U.S. Treasury Wally Adeyemo, *The National*, "[Houthi actions are hurting the people of the region and hopes for Red Sea prosperity](#)" (Mar. 18, 2024).
8. See Treasury, "[Treasury Sanctions Hamas-Aligned Terrorist Fundraising Network](#)" (Mar. 27, 2024), and "[Treasury Targets Qods Force, Houthi, and Hizballah Finance and Trade Facilitators](#)" ("Mar. 2024 Treasury Press Release") (Mar. 26, 2024). See also Treasury, "[Remarks by Deputy Secretary of the Treasury Wally Adeyemo at the Royal United Services Institute in London, the United Kingdom](#)" (Oct. 27, 2023), and "[Under Secretary for Terrorism and Financial Intelligence Brian Nelson to Travel to the Middle East](#)" (Oct. 22, 2023).
9. FinCEN, "[Anti-Money Laundering and Countering the Financing of Terrorism National Priorities](#)" (Jun. 30, 2021). See also Treasury, "[2024 National Terrorism Financing Risk Assessment](#)" ("Feb. 2024 Terrorism Risk Assessment") (Feb. 2024).
10. The IRGC was designated by Treasury as a SDGT on October 13, 2017, pursuant to EO 13224. It was added to the U.S. Department of State's FTO list on April 15, 2019. See Treasury, "[Treasury Designates the IRGC under Terrorism Authority and Targets IRGC and Military Supporters under Counter-Proliferation Authority](#)" (Oct. 13, 2017). See also Department of State, "[Designation of the Islamic Revolutionary Guard Corps](#)" (Apr. 8, 2019).
11. The IRGC-QF was designated by Treasury as a SDGT on October 25, 2007, pursuant to EO 13224. See OFAC, "[Global Terrorism \(SDGT\) Designations and NPWMD Designations](#)" (Oct. 25, 2007), and "[Treasury and the United Kingdom Target Qods Force Deputy Commander and Houthi-Affiliated Supporters](#)" (Feb. 27, 2024).
12. See Jan. 2024 CRS Report, *supra* note 2 at p. 4.

Iran's Sources of Foreign Revenue

Iran uses the revenue from the sale of commodities, particularly oil, to countries such as the People's Republic of China (PRC) to fund its terrorist proxies.¹³ Following the reimposition of U.S. sanctions against Iran's petroleum sector in 2018,¹⁴ Iran's ability to finance itself through sales of crude oil and petroleum products—its most important economic sector—was severely diminished. In response, Iran established large-scale global oil smuggling and money laundering networks to enable access to foreign currency and the international financial system through the illicit sale of crude oil and petroleum products in global markets.¹⁵

In 2021, the National Iranian Oil Company sold approximately \$40 billion worth of products,¹⁶ and its crude oil and condensate exports reached an average of more than 600,000 barrels per day, with nearly all of it sent to the PRC and Syria.¹⁷ Iran's exports to the PRC have increased over time, reaching approximately 1.3 million barrels per day in 2023.¹⁸ Some of these oil proceeds finance the activities of the IRGC-QF and other terrorist groups.¹⁹ To restrict these sources of revenue, Treasury has designated numerous Iranian- and third-country operatives, front companies, and ships involved in Iran's oil smuggling networks.²⁰

13. See Treasury, "[Treasury Sanctions Key Actors in Iran's Oil Sector for Supporting Islamic Revolutionary Guard Corps-Qods Force](#)" (Oct. 26, 2020). See also Jan. 2024 CRS Report, *supra* note 2 at p. 15.
14. As part of the reimposition of U.S. nuclear-related sanctions that had been lifted or waived in connection with the Joint Comprehensive Plan of Action (JCPOA), Treasury designated over 400 persons and entities connected to the Iranian energy and shipping sectors. See Treasury, "[U.S. Government Fully Re-Imposes Sanctions on the Iranian Regime as Part of Unprecedented U.S. Economic Pressure Campaign](#)" (Nov. 5, 2018).
15. See, e.g., Treasury, "[Treasury Sanctions Companies Involved in the Production, Sale, and Shipment of Iranian Petrochemicals and Petroleum](#)" (Feb. 9, 2023); "[Treasury Targets Network Supporting Iranian Petrochemical and Petroleum Sales](#)" (Nov. 17, 2022), and "[Treasury Targets Companies Supporting Iranian Petrochemical Conglomerate](#)" (Aug. 1, 2022).
16. U.S. Energy Information Agency (EIA), "[Country Analysis Executive Summary: Iran](#)" ("Nov. 2022 EIA Country Analysis") (Nov. 17, 2022), at p. 2.
17. *Id.*, at p. 5. See also Jan. 2024 CRS Report, *supra* note 2 at Summary and p. 13. In 2019, Treasury designated actors involved in a large shipping network that is directed by the IRGC-QF and Hizballah that moved oil worth hundreds of millions of dollars for the benefit of the Assad regime in Syria, Hizballah, and other illicit actors. In spring 2019 alone, this IRGC-QF-led network employed more than a dozen vessels to transport nearly 10 million barrels of crude oil, predominantly to the Syrian regime. See Treasury, "[Treasury Designates Vast Iranian Petroleum Shipping Network that Supports IRGC-QF and Terror Proxies](#)" (Sept. 4, 2019).
18. See CRS, "[Iran's Petroleum Exports to China and U.S. Sanctions](#)" (Feb. 28, 2024), at p. 2.
19. See Treasury, "[Treasury Targets Vessels Shipping Iranian Commodities for Houthis and Qods Force](#)" (Mar. 15, 2024).
20. See, e.g., Treasury, "[Treasury Sanctions Oil Shipping Network Supporting IRGC-QF and Hizballah](#)" ("Nov. 2022 Treasury Press Release") (Nov. 3, 2022); "[Treasury Sanctions Network Financing Houthi Aggression and Instability in Yemen](#)" ("June 2021 Treasury Press Release") (June 10, 2021); "[Treasury Targets Oil Smuggling Network Generating Hundreds of Millions of Dollars for Qods Force and Hizballah](#)" (May 25, 2022); and "[Treasury Targets Companies and Vessels Facilitating Qods Force and Houthi Commodity Shipments](#)" (Mar. 6, 2024).

Proceeds from Iran's sale of weapons and unmanned aerial vehicles (UAVs), including to buyers in Russia, also benefit the Iranian military, including the IRGC-QF.²¹ In response, Treasury has also designated companies that enable Iran's UAV production.²²

Case Study

In February 2024, the U.S. Department of Justice (DOJ) indicted seven defendants, including a senior IRGC-QF official and officers of a Turkish energy group, on terrorism, sanctions evasion, fraud, and money laundering charges in connection with their illicit billion-dollar network that enabled Iran to sell its oil products to government-affiliated buyers in the PRC, Russia, and Syria and to gain access to foreign currency. The United States seized \$108 million that China Oil & Petroleum Limited, a Hong Kong-based IRGC front company,²³ attempted to launder through correspondent transaction accounts at U.S. financial institutions in furtherance of the scheme to fund the IRGC-QF's malign activities through the illicit sale of Iranian oil. In furtherance of this scheme, the defendants charged in the U.S. District Court for the Southern District of New York used a myriad of deceptive techniques including: (1) the use of front companies and intermediaries in countries outside of Iran to disguise the IRGC's role in the oil transactions and the Iranian source of the oil; (2) the use of falsified documentation to misrepresent the source of the oil and deceive unwitting companies and banks to provide services in furtherance of the scheme; and (3) the use of ship-to-ship transfers and the manipulation of location and shipping data for vessels to obscure the loading and unloading of Iranian oil cargoes and therefore avoid identifying vessels used to facilitate oil smuggling.

Likewise, defendants charged in a related U.S. District Court for the District of Columbia indictment allegedly negotiated the sale of and sold illicit Iranian oil to buyers in the PRC. They allegedly obtained the oil from Iran using surreptitious means, and the scheme relied on the use of the U.S. financial system. According to the indictment, the defendants created fraudulent documents to mask the oil's Iranian origin, used electronic communications to arrange for

21. The IRGC-QF maintains a division known as Department 8000 tasked with developing UAVs and providing UAVs and UAV-related training to proxy forces such as the Houthis in Yemen and Iranian-aligned militia groups in Iraq and Syria. Iranian-manufactured UAVs have been provided to and utilized by Iran-backed militias across the Middle East, resulting in attacks against U.S. service members, allied forces, maritime vessels in the Red Sea. See Treasury, ["Treasury Targets Iranian UAV Program, Steel Industry, and Automobile Companies in Response to Unprecedented Attack on Israel"](#) (Apr. 18, 2024). See also Jan. 2024 CRS Report, *supra* note 2 at Summary, p. 7.
22. See, e.g., Treasury, ["Treasury Targets Vessel Shipping Iranian Commodities Valued at over \\$100 Million for Iran's Ministry of Defense"](#) (Feb. 27, 2024); ["Treasury Targets Actors Involved in Production and Transfer of Iranian Unmanned Aerial Vehicles to Russia for Use in Ukraine"](#) (Nov. 15, 2022); ["Treasury Sanctions Iranian Persons Involved in Production of Unmanned Aerial Vehicles and Weapon Shipment to Russia"](#) (Sept. 8, 2022); and ["Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military"](#) (Apr. 25, 2024).
23. Treasury's Office of Foreign Assets Control (OFAC) sanctioned China Oil & Petroleum Limited on the same day the DOJ unsealed the indictment for its role arranging contracts, selling hundreds of millions of dollars' worth of Iranian commodities for the benefit of the IRGC-QF, and using falsified documents to mask the origin of the Iranian commodities. See Treasury, ["Treasury Sanctions Transnational Procurement Network Supporting Iran's Ballistic Missile and UAV Programs"](#) ("Feb. 2, 2024 Treasury Press Release") (Feb. 2, 2024); DOJ, ["Justice Department Announces Terrorism and Sanctions-Evasion Charges and Seizures Linked to Illicit, Billion-Dollar Global Oil Trafficking Network That Finances Iran's Islamic Revolutionary Guard Corps and Its Malign Activities"](#) ("Feb. 2024 DOJ Press Release") (February 2, 2024).

Chinese buyers, used shell corporations to launder the proceeds through the U.S. financial system, provided false information to the U.S. companies about the source of funds generated by the transactions, and used U.S. companies as a “trust” to hold the profits for the IRGC.²⁴

Moving the Money

Iranian government agencies, such as the Central Bank of Iran (CBI) and the IRGC-QF, as well as state-sponsored organizations such as Hizballah, play a key role in channeling funds to terrorist proxies using overseas front companies and financial institutions.²⁵ Financial institutions located outside Iran can—wittingly or unwittingly—become intermediaries for the IRGC-QF’s illicit transactions.²⁶ IRGC-QF officials have been known to collect funds in various currencies from CBI-held accounts at financial institutions in neighboring countries and transfer those funds back to Iran or to terrorist organizations.²⁷ According to BSA analysis, third-country front companies—often incorporated as “trading companies” or “general trading companies”—and exchange houses²⁸ act as a global “shadow banking” network that processes illicit commercial transactions and channels money to terrorist organizations on Iran’s behalf.²⁹ Exchange houses and front companies rely on banks with correspondent accounts with U.S. financial institutions, especially to process dollar-denominated transactions. In such cases, Iranian banking customers may omit

24. See Feb. 2024 DOJ Press Release, *supra* note 23.

25. A front company is a legal entity used to obscure the identity of the owner or the true nature of their business activities. See Treasury, [“Treasury Targets Iran’s Central Bank Governor and an Iraqi Bank Moving Millions for IRGC-Qods Force”](#) (May 15, 2018); [“Treasury Sanctions Iran’s Central Bank and National Development Fund”](#) (“Sept. 2019 Treasury Press Release”) (Sept. 20, 2019); [“United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF”](#) (May 10, 2018); [“Terrorist Financing Targeting Center Jointly Designates Network of Corporations, Banks, and Individuals Supporting IRGC and Hizballah”](#) (“Oct. 2019 Treasury Press Release”) (Oct. 30, 2019); and June 2021 Treasury Press Release, *supra* note 20. See also Oct. 2018 FinCEN Advisory, *supra* note 1 at pp. 2-4.

26. On January 29, 2024, FinCEN issued a finding and notice of proposed rulemaking (NPRM) that identified Al-Huda Bank, an Iraqi bank that serves as a conduit for terrorist financing, as a foreign financial institution of primary money laundering concern. Along with its finding, FinCEN proposed imposing a special measure that would sever the bank from the U.S. financial system by prohibiting domestic financial institutions and agencies from opening or maintaining a correspondent account for or on behalf of Al-Huda Bank. Since its establishment, Al-Huda Bank has been controlled and operated by the IRGC and the IRGC-QF and has laundered money and afforded access to the U.S. financial system for the IRGC-QF and Kata’ib Hizballah (KH) and Asa’ib Ahl al-Haq (AAH). See FinCEN, [“FinCEN Finds Iraq-based Al-Huda Bank to be of Primary Money Laundering concern and Proposes a Rule to Combat Terrorist Financing”](#) (“Jan. 2024 FinCEN Press Release”) (Jan. 29, 2024). OFAC also designated Hamad al-Moussawi, the owner and president of the board of directors of Iraq’s Al-Huda Bank, for his support to the IRGC-QF, including through support for its proxy militia groups in Iraq. See Treasury, [“U.S. Treasury Takes Action to Protect Iraqi Financial System from Abuse”](#) (Jan. 29, 2024).

27. See Sep. 2019 Treasury Press Release, *supra* note 25.

28. An exchange house is an entity specializing in the purchase and sale of foreign currency which derives its profits from differences in exchange rates and currency sales. For more information about Iran’s use of exchange houses, see OFAC, [“Advisory on the Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran”](#) (Jan. 10, 2013).

29. A shadow bank is a non-bank financial service provider that performs functions like a bank outside of regulatory oversight. On March 9, 2023, OFAC sanctioned 39 entities constituting a significant “shadow banking” network, one of several multi-jurisdictional illicit finance systems which grant sanctioned Iranian entities access to the international financial system and obfuscate their trade with foreign customers. See Treasury, [“Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime”](#) (Mar. 9, 2023). See also Treasury, [“Treasury Designates Vast Network of IRGC-QF Officials and Front Companies in Iraq, Iran”](#) (“Mar. 2020 Treasury Press Release”) (Mar. 26, 2020).

or falsify identifying details connecting themselves or the transfers to Iran or attempt to pass the transactions off as remittances.³⁰

In addition, Iran uses cultural and religious foundations as front organizations for funneling money to terrorist organizations under the guise of cultural or religious support. In 2020, Treasury sanctioned the Reconstruction Organization for the Holy Shrines in Iraq (ROHSI).³¹ Ostensibly a religious institution devoted to restoring and preserving Shiite shrines in Iraq, ROHSI is in reality an IRGC-QF front organization that channels funds to terrorist organizations.³²

Typologies Associated with Iran-Backed Terrorist Organizations

In addition to receiving support from Iran, terrorist organizations and Iran-aligned militia groups in Iraq and Syria employ a range of other mechanisms to raise revenue, including sham or fraudulent charities, engaging in illicit trade activities like arms and drug trafficking, taxing and extorting local populations, and crowdfunding.

*Hamas*³³

Hamas is a Sunni terrorist organization based predominantly in the Gaza Strip whose goal is the destruction of Israel and its replacement with an Islamic Palestinian state.³⁴ Hamas has exercised *de facto* control over Gaza since 2007, which enabled the group to derive revenue from taxes and fees it imposed on the local population. Until October 2023, Hamas levied taxes on commodities, imports, and businesses operating in Gaza, and charged fees for licenses, birth certificates, customs duties, and vehicles.³⁵ This source of revenue has effectively disappeared since the October 7, 2023, attacks on Israel and ongoing armed conflict in Gaza, leaving Hamas largely dependent on support from Iran, crowdfunding contributions, and whatever revenue the group can generate from its investment portfolio.³⁶

Hamas and its armed element, the Al-Qassam Brigades, have received support from Iran since the 1990s³⁷ through networks of corporations, banks, and individuals located in multiple countries, including the People's Democratic Republic of Algeria (Algeria), the Republic of Lebanon (Lebanon), the Kingdom of Saudi Arabia (Saudi Arabia), the Republic of Sudan (Sudan), the Republic of Türkiye (Türkiye), and the United Arab Emirates (UAE), that help transfer money

30. See Oct. 2018 FinCEN Advisory, *supra* note 1 at p. 4.

31. See Mar. 2020 Treasury Press Release, *supra* note 29.

32. *Id.*

33. FinCEN published an alert in October 2023 to help financial institutions identify and report suspicious activity connected to Hamas. See FinCEN, "[FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities](#)" ("Oct. 2023 FinCEN Alert") (Oct. 20, 2023).

34. See Feb. 2024 Terrorism Risk Assessment, *supra* note 9 at p. 14.

35. U.S. Senate Committee on Banking, Housing, and Urban Affairs, Testimony by Dr. Matthew Levitt, "[Combating the Networks of Illicit Finance and Terrorism](#)" ("Oct. 2023 Levitt Testimony") (Oct. 26, 2023), at p.3.

36. Prior to the imposition of U.S. sanctions in May 2022, this portfolio was worth an estimated \$500 million and included companies operating in Algeria, Saudi Arabia, Sudan, Türkiye, and the UAE. See Treasury, "[Treasury Targets Covert Hamas Investment Network and Finance Official](#)" ("May 2022 Treasury Press Release") (May 24, 2022).

37. CRS Report, "[Israel and Hamas October 2023 Conflict: Frequently Asked Questions \(FAQs\)](#)" (Oct. 20, 2023), at pp. 12-13.

directly to Hamas.³⁸ Iran has provided as much as \$100 million per year to Hamas since 2018.³⁹ To disrupt these sources of support, Treasury has sanctioned numerous financial intermediaries between Iran and Hamas, including money transfer companies, financiers and financial facilitators who manage Hamas's assets and facilitate money transfers for the organization, and political liaisons to the Government of Iran.⁴⁰

Hamas also has a history of using "sham" charities: usually foreign non-profit organizations (NPOs) that claim to provide humanitarian assistance but instead primarily or exclusively funnel money to terrorist organizations, exploiting the trust and credibility associated with charitable giving.⁴¹ In addition, Hamas and other terrorist groups have exploited crowdfunding and social media platforms to raise funds under the guise of humanitarian or charitable causes worldwide.⁴² According to analysis of BSA data, these donations are often placed in bank accounts in third countries, including Lebanon, the State of Qatar (Qatar), and Türkiye, which are then accessed by individuals operating in the Gaza Strip.

Additionally, Hamas has used convertible virtual currency (CVC) for fundraising, leveraging money exchangers that have incorporated CVC into their operations to facilitate cross-border transfers, probably seeking to benefit from the perceived anonymity afforded by certain CVC transactions and the lax regulatory oversight of virtual asset service providers (VASPs) in some high-risk jurisdictions.⁴³ Hamas has sought CVC contributions in donation drives since at least

38. See May 2022 Treasury Press Release, *supra* note 36.

39. See Feb. 2024 Terrorism Risk Assessment, *supra* note 9 at p. 14. See also Treasury, "[Treasury Targets Network Moving Millions to HAMAS in Gaza](#)" (Aug. 29, 2019). Despite this consistent support, Office of the Director of National Intelligence (ODNI) assessed that Iran did not have foreknowledge of Hamas's October 7, 2023, attacks on Israel. See ODNI, "[Annual Threat Assessment of the U.S. Intelligence Community](#)" (Feb. 5, 2024), at p. 24.

40. See Treasury, "[Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators](#)" (Oct. 18, 2023). To date, Treasury has targeted nearly 1,000 individuals and entities connected to terrorism and terrorist financing by the Government of Iran and its proxies, including Hamas, Hizballah, and other Iran-aligned terrorist groups in the region. See Department of State, Press Statement by Antony Blinken, U.S. Secretary of State, "[Designating Hamas Operatives and Financial Facilitators - United States Department of State](#)" (Oct. 18, 2023). See also Treasury, "[Treasury Targets Additional Sources of Support and Financing to Hamas](#)" ("Oct. 2023 Treasury Press Release") (Oct. 27, 2023).

41. See Feb. 2024 Terrorism Risk Assessment, *supra* note 9 at p. 24. Treasury remains committed to denying Hamas access to funds following its heinous terrorist attacks against the people of Israel, while also ensuring legitimate humanitarian aid can continue to flow to the Palestinian people in Gaza. To that end, and consistent with longstanding policy to issue general licenses to authorize transactions in support of humanitarian relief efforts, OFAC authorizes limited transactions with blocked persons to the extent such dealings are ordinarily incident and necessary to certain humanitarian activity. See OFAC, "[Guidance for the Provision of Humanitarian Assistance to the People of Gaza](#)" ("Nov. 2023 OFAC Compliance Communique") (Nov. 14, 2023).

42. For example, shortly after the October 7, 2023, attacks, the pro-Hamas news outlet *Gaza Now* began disseminating fundraising information on social media. Cloaked in the language of humanitarian aid, these fundraisers mislead donors as to the end use of their contributions, which were ultimately funneled to Hamas. These campaigns solicited donations in dollars, euros, and cryptocurrency and touched the U.S. and European banking systems. Other recent crowdfunding campaigns intended to support Hamas include those set up by the U.K.-based Al-Qureshi Executives, the U.K.- and Türkiye-based Al Khair Foundation, and Kudus Vakfi, an NGO based in Türkiye and run by senior leadership of the U.S.-sanctioned Al Aqsa Foundation. See Oct. 2023 Levitt Testimony, *supra* note 35 at p. 8.

43. According to FinCEN analysis of BSA information, between January 2020 and October 2023, financial institutions reported approximately \$165 million in suspicious activity filings related to Hamas and CVC involving over 200 unique CVC addresses. Given that filing institutions frequently attribute the full value of a customer's transactions—including both fiat and CVC activity—to Hamas, even when only a portion of the reported activity may be related, the reported value is likely an overestimate.

2019,⁴⁴ and has historically leveraged VASPs in an attempt to safeguard the anonymity of their donors.⁴⁵ There is evidence, however, that Hamas has reacted to law enforcement action targeting its use of CVC. For instance, in April 2023, the al-Qassam Brigades announced that they would no longer accept Bitcoin donations, warning that donors could be targeted.⁴⁶

Houthis

The Houthis, or Ansarallah, are an Iran-backed Zaidi Islamist⁴⁷ movement that arose in Northern Yemen in 2004. In 2014, the Houthis launched a military campaign to overthrow the internationally recognized Yemeni government, initiating a bloody civil war. Today, the Houthis control a large portion of northern Yemen, including the former capital, Sana'a.⁴⁸

Following the Hamas attacks on Israel on October 7, 2023, the Houthis began attacking commercial and naval vessels transiting the Red Sea and Gulf of Aden. Since October 17, 2023, the Houthis have carried out more than 50 attacks on commercial vessels, forcing companies to divert their shipments to the much costlier route around Africa's Cape of Good Hope.⁴⁹ In response, the U.S. Department of State redesignated the Houthis as a Specially Designated Global Terrorist (SDGT), effective February 16, 2024.⁵⁰ The United States has also responded by launching Operation Prosperity Guardian, a naval coalition of more than 20 countries to protect commercial vessels;⁵¹ by leading a coalition that has conducted a series of strikes against Houthi targets in Yemen;⁵² and by imposing sanctions against the exchange houses and smuggling network through which Iran funds the Houthis.⁵³

44. In August 2020, the DOJ, Federal Bureau of Investigation (FBI), Treasury, and Internal Revenue Service-Criminal Investigations (IRS-CI) collaborated to dismantle three Bitcoin funding campaigns benefiting terrorist organizations, including one initiated by Hamas' al-Qassam Brigades. The fundraiser was advertised using social media and the al-Qassam website and falsely claimed that Bitcoin contributions were untraceable. U.S. authorities seized the website infrastructure and all 150 Bitcoin wallets that had helped launder the funds and charged two foreign nationals with money laundering in connection with the campaign. See CRS, "[Terrorist Financing: Hamas and Cryptocurrency Fundraising](#)" ("Nov. 2023 CRS In Focus") (Nov. 27, 2023), at p. 1; see also, DOJ, "[Global Disruption of Three Terror Finance Cyber-Enabled Campaigns](#)" (Aug. 13, 2020).

45. In November 2023, FinCEN and OFAC entered a \$3.4 billion settlement with VASP Binance, in part due to its failure to identify and report suspicious transactions involving terrorist organizations including PIJ and Hamas' al-Qassam Brigades. See Treasury, "[U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws](#)" (Nov. 21, 2023).

46. See Nov. 2023 CRS In Focus, *supra* note 44 at p. 1.

47. Zaydism is a distinct form of Shi'a Islam practiced by 35% of the Yemeni population. Its similarity to Shi'a Islam is a large reason for Iran's support of the Ansarallah movement, despite its distinction from the Islam dominant in Iran. See Department of State, "[2020 Report on International Religious Freedom: Yemen](#)" (May 12, 2021).

48. CRS, "[Houthi Attacks in the Red Sea: Issues for Congress](#)" ("Jan. 2024 CRS Insight") (Jan. 31, 2024), at p.2.

49. *Id.*

50. See Jan. 2024 Houthi Designation, *supra* note 6. In conjunction with this designation, Treasury issued six general licenses to ensure humanitarian assistance to the Yemeni people. See OFAC, "[Guidance for the Provision of Humanitarian-Related Assistance and Critical Commodities to the Yemeni People](#)" (Feb. 16, 2024). The Houthis were briefly designated by the U. S. Department of State as an SDGT in 2021, however the designation was revoked in recognition of the dire humanitarian situation in Yemen. See Department of State, "[Terrorist Designation of Ansarallah in Yemen](#)" (Jan. 10, 2021). See also Department of State, "[Revocation of the Terrorist Designations of Ansarallah](#)" (Feb. 12, 2021).

51. See Jan. 2024 CRS Insight, *supra* note 48 at p. 3.

52. Department of Defense, "[U.S., U.K. Launch Strikes Against Houthi Targets in Yemen to Protect Red Sea Shipping](#)" (Feb. 4, 2024).

53. Treasury, "[Treasury Targets Network Financing Houthi Attacks on International Shipping](#)" (Dec. 28, 2023).

Much of the Houthis' funding is raised and transferred by means of an elaborate smuggling network connected to Iran-based IRGC-QF-backed Houthi financial facilitator Said Al-Jamal. The network generates tens of millions of dollars in revenue annually through the sale of Iranian commodities like petroleum to customers in Asia, the Middle East, and Africa. Those funds are then funneled to the Houthis in Yemen through a complex network of exchanges and intermediaries spread across multiple countries. Al-Jamal also maintains connections to Hizballah and has worked with the group to send millions of dollars to benefit the Houthis.⁵⁴ The Houthis also raise funds by collecting customs revenue from the Hudaydah and Salif ports in Yemen, appropriating public funds using fraudulent contracts, and unlawfully appropriating assets belonging to political opponents or those who have fled the country.⁵⁵

Hizballah

Formed in the wake of Israel's invasion of Lebanon in 1982, Hizballah is a strategic partner through which Iran projects power throughout the Middle East. While primarily based in Lebanon, Hizballah's activities extend to Syria, Iraq, and Yemen.⁵⁶ Iran has provided hundreds of millions of dollars in support to Hizballah and has trained thousands of its fighters at camps in Iran. Hizballah in turn has trained and equipped other Iran-aligned militias in the region and acts as a conduit for funds from Iran's IRGC-QF to other Iran-aligned groups.⁵⁷

Estimates indicate that Iran has historically provided Hizballah with approximately \$700 million of Hizballah's estimated \$1 billion annual budget.⁵⁸ While Iran has supported Hizballah and others through a vast network of front companies, banks, and individuals,⁵⁹ Hizballah also finances itself through a broad range of illicit activities, including oil smuggling,⁶⁰ money laundering, drug trafficking,⁶¹ counterfeiting, and illegal weapons procurement.⁶² These activities are global in scale,

54. See June 2021 Treasury, *supra* note 20.

55. United Nations Security Council, "[Final report of the Panel of Experts on Yemen](#)" (Jan. 27, 2020), at pp. 28-32.

56. CRS, "[Lebanese Hezbollah](#)" ("Jan. 2023 CRS Report") (Jan. 11, 2023), at pp. 1-2.

57. *Id.*, at p. 2.

58. Treasury, "[Treasury and State Announce New Humanitarian Mechanism to Increase Transparency of Permissible Trade Supporting the Iranian People](#)" (Oct. 25, 2019).

59. See Oct. 2019 Treasury, *supra* note 25. See also Treasury, "[Treasury Labels Bank Providing Financial Services to Hizballah as Specially Designated Global Terrorist](#)" (Aug. 29, 2019).

60. In 2022, Treasury sanctioned a Hizballah and IRGC-QF oil smuggling network that blended Iranian oil with Indian oil and used modified or counterfeit certificates to obfuscate its origins. See Nov. 2022 Treasury Press Release, *supra* note 20. Furthermore, in 2019, OFAC issued an advisory alerting to sanctions risk of vessels carrying petroleum from Iran have been known to intentionally disable their AIS transponders or modify transponder data to mask their movements and have engaged in ship-to-ship transfers to conceal the origin or destination of their cargo. See OFAC, "[OFAC Advisory to the Maritime Petroleum Shipping Community](#)" (Sept. 4, 2019).

61. Hizballah's External Security Organization Business Affairs Component (BAC) has established partnerships with South American drug trafficking organizations and is responsible for the movement of large quantities of cocaine into U.S. and European markets. A Drug Enforcement Administration (DEA) investigation in 2015 uncovered a large network of Hizballah-affiliated money carriers that transported drug proceeds from Europe to the Middle East that were then disbursed to Colombian drug traffickers through the hawala system. Much of this money transited through Lebanon and a significant portion benefited Hizballah. See DEA, "[DEA And European Authorities Uncover Massive Hizballah Drug And Money Laundering Scheme](#)" (Feb. 1, 2016).

62. Treasury, "[2022 National Terrorist Financing Risk Assessment](#)" ("Feb. 2022 Terrorism Risk Assessment") (Feb. 2022), at p. 10.

encompassing the western hemisphere, Europe, Africa, and the Middle East, and often have a nexus to transnational organized criminal groups, drug trafficking organizations, and professional money laundering organizations.⁶³

Hizballah also utilizes networks of front companies and legitimate businesses,⁶⁴ as well as cryptocurrencies,⁶⁵ to raise, launder, and transfer funds.⁶⁶ Hizballah financiers make use of free trade zones and countries with weak regulatory frameworks to establish import-export companies that facilitate trade-based money laundering schemes. These companies are often held in the name of a relative of the financier, for example a spouse. Hizballah operatives have been known to operate in the Tri-border area of Argentina, Brazil, and Paraguay, and in free trade zones in Chile and Panama, with members and supporters identified in Colombia and Peru as well.⁶⁷ Hizballah's illicit activities also extend to Africa. In 2019, Treasury designated Nazem Said Ahmad, who had used his Africa-based diamond business to launder money on behalf of Hizballah,⁶⁸ along with Saleh Assi, who used his Congo-based businesses to launder and raise funds for Hizballah.⁶⁹

Palestinian Islamic Jihad

PIJ is a Sunni Islamist terrorist organization operating in Gaza and the West Bank. It is the second-largest armed group in Gaza and receives support from Iran, Syria, and Hizballah. PIJ and Hamas share many similarities: both are violent offshoots of the Muslim Brotherhood; both seek to create an Islamic Palestinian state through the destruction of Israel; and both receive significant funding and support from Iran.⁷⁰ Like Hamas and Hizballah, PIJ's operatives have been trained by Iran to use Iranian-made missiles for long-range rocket attacks against Israeli cities and to carry out suicide bombings.⁷¹

63. See Feb. 2024 Terrorism Risk Assessment, *supra* note 9 at pp. 12-13.

64. *Id.*

65. In March 2024, Treasury sanctioned Lebanon-based Syrian money exchanger Tawfiq Muhammad Sa'id al-Law for providing Hizballah with digital wallets to receive funds from IRGC-QF commodity sales and for conducting cryptocurrency transfers on behalf of the sanctioned Syrian Qatirji Company, sanctioned Hizballah officials, and Sa'id al-Jamal and his network. See Mar. 2024 Treasury Press Release, *supra* note 8.

66. See Feb. 2024 Terrorism Risk Assessment, *supra* note 9 at p. 12.

67. Department of State, "[Country Reports on Terrorism 2021](#)" ("2021 State Country Reports") (2021), at p. 191. See also Treasury, "[Treasury Designates Hizballah Operatives and Financial Facilitators in South America and Lebanon](#)" (Sept. 12, 2023).

68. A nine-count indictment was unsealed on April 18, 2023, in the United States District Court for the Eastern District of New York charging Ahmad and eight co-defendants with conspiring to defraud the United States and foreign governments, evade U.S. sanctions and customs laws, and conduct money laundering transactions by securing goods and services for the benefit of Ahmad. Despite being sanctioned since December 2019, Ahmad and his coconspirators relied on a complex web of business entities to obtain valuable artwork from U.S. artists and art galleries and to secure U.S.-based diamond-grading services all while hiding Ahmad's involvement in and benefit from these activities. Approximately \$160 million worth of artwork and diamond-grading services were transacted through the U.S. financial system. See DOJ, "[OFAC-Designated Hizballah Financier and Eight Associates Charged with Multiple Crimes Arising Out of Scheme to Evade Terrorism-Related Sanctions](#)" (Apr. 18, 2023).

69. See Feb. 2022 Terrorism Risk Assessment, *supra* note 62 at p. 11.

70. Treasury designated three PIJ members, two of whom serve as liaisons to Iran, along with a foundation used to provide financial support to the families of PIJ fighters and prisoners in November 2023. See Treasury, "[United States and United Kingdom Take Coordinated Action Against Hamas Leaders and Financiers](#)" ("Nov. 2023 Treasury Press Release") (Nov. 14, 2023). See also Feb. 2023 Counter Terrorism Guide, *supra* note 5.

71. See 2021 State Country Reports, *supra* note 67 at pp. 139, 302-303.

PIJ relies on many of the same funding channels as Hamas. It receives much of its support from the IRGC and IRGC-QF, which distribute those funds through PIJ intermediaries or through Islamic National Bank of Gaza, which was designated by Treasury in 2010 for being controlled by Hamas.⁷² Also like Hamas, PIJ makes use of sham charities to move and launder funds. In 2023, Treasury sanctioned the Al-Ansar Charity Foundation and the Muhjat al-Quds Foundation, through which Iran provided financial support to PIJ fighters and their families.⁷³

Iran-aligned Militia Groups in Iraq and Syria

Some of the most prominent Iran-aligned militia groups in Iraq are Kata'ib Hizballah (KH),⁷⁴ Kata'ib Sayyid al Shuhada (KSS),⁷⁵ Asa'ib Ahl al-Haq (AAH),⁷⁶ and Harakat al-Nujaba (HaN).⁷⁷ These groups have received support, training, weapons, and intelligence from the IRGC-QF and Hizballah. These groups have also abused the Iraqi financial system to generate revenue and launder money, including through the use of front companies, fraudulent documentation, identity theft, currency arbitrage, and counterfeit currency.⁷⁸ Although some members of Iran-aligned militia groups operate within Iraq's official Popular Mobilization Forces (PMF), these groups frequently operate outside government control and conduct destabilizing attacks in Iraq and neighboring Syria⁷⁹ as well as attacks against coalition forces seeking to defeat the Islamic State of Iraq and Syria (ISIS).⁸⁰

72. See Oct. 2023 Treasury Press Release, *supra* note 40. See also Treasury, "[Treasury Designated Gaza-Based Business, Television Station for Hamas Ties](#)" (Mar. 18, 2010).

73. See Oct. 2023 Treasury Press Release, *supra* note 40. See also Nov. 2023 Treasury Press Release, *supra* note 70.

74. While unconfirmed, the U.S. Department of Defense has speculated that the UAV attack in Jordan on January 28, 2024, that killed three U.S. servicemen and injured 40 more was the work of Kita'ib Hizballah. See Department of Defense, "[3 U.S. Service Members Killed, Others Injured in Jordan Following Drone Attack](#)" (Jan. 29, 2024). KH was designated as an FTO on July 2, 2009, by the Secretary of State in accordance with section 219 of the INA, as amended, and as a SDGT pursuant to EO 13224 on July 2, 2009. For more information about KH, see DNI NCTC, "[Counter Terrorism Guide: Kita'ib Hizballah \(KH\)](#)" (Sept. 2022).

75. KSS was designated by Treasury as a SDGT pursuant to EO 13224 on November 17, 2023. See Treasury, "[Treasury Sanctions Iran-Aligned Militias in Iraq](#)" (Nov. 17, 2023).

76. Asa'ib al-Haq (AAH) was designated as an FTO on January 10, 2020 by the Secretary of State in accordance with section 219 of the INA, as amended, and as a SDGT pursuant EO 13224 on January 3, 2020. For more information about AAH, see DNI NCTC, "[Counter Terrorism Guide: Asa'ib alh-Haqq \(AAH\)](#)" (Sept. 2022).

77. HaN was designated as a SDGT pursuant to EO 13224 on March 5, 2019. See Treasury, "[Counter Terrorism Designation and Designation Update](#)" (Mar. 5, 2019).

78. See Jan. 2024 FinCEN Press Release, *supra* note 26. See also Treasury, "[Treasury Targets Kata'ib Hizballah Leaders and Airline Enabling IRGC-QF and Militant Proxy Groups](#)" (Jan. 22, 2024).

79. Department of State, "[Country Reports on Terrorism 2022: Iraq](#)" (2022).

80. ISIS's predecessor, Al-Qaeda in Iraq (AQI), was designated as an FTO in December 2004 in accordance with section 219 of the INA, as amended, and this designation remains in effect for ISIS. For more information about ISIS, see DNI NCTC, "[Counter Terrorism Guide: Islamic State of Iraq and Ash-Sham \(ISIS\)](#)" (Sept. 2022). As of late January 2024, Iran-backed groups have reportedly attacked U.S. forces in Iraq and Syria 140 times since October 17, 2023 (52 times in Iraq, 75 in Syria); media sources affiliated with the "Islamic Resistance in Iraq," a catch-all descriptor for Iran-backed Iraqi militia groups operating in Iraq and Syria, have claimed many of these actual or attempted assaults. These attacks have mostly used one-way attack drones and rockets, but also include at least one short-range ballistic missile attack. Those attacks have left "nearly 70" U.S. personnel injured, with most returning to duty "in short order," per the Pentagon. See Jan. 2024 CRS Report, *supra* note 2 at p. 6.

Red Flag Indicators Related to the Fundraising and Money Laundering Activities of Iran-Backed Terrorist Organizations

FinCEN has identified the red flags listed below to assist financial institutions in detecting, preventing, and reporting suspicious activity connected to the financing of Iran-backed terrorist organizations. These red flags are in addition to the red flags identified in FinCEN's 2018 Iran advisory⁸¹ and 2023 Hamas alert,⁸² all of which remain relevant. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding 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 if a behavior or transaction is indicative of terrorist finance or is otherwise suspicious.

-  1 A customer or a customer's counterparty conducts transactions with Office of Foreign Assets Control (OFAC)-designated entities and individuals, or transactions that contain a nexus to identifiers listed for OFAC-designated entities and individuals, to include email addresses, physical addresses, phone numbers, passport numbers, or CVC addresses.
-  2 Information included in a transaction between customers or in a note accompanying a peer-to-peer transfer include key terms known to be associated with terrorism or terrorist organizations.
-  3 A customer conducts transactions with a money services business (MSB) or other financial institution, including a VASP, that operates in jurisdictions known for, or at high risk for, terrorist activity and is reasonably believed to have lax customer identification and verification processes, opaque ownership, or otherwise fails to comply with AML/CFT best practices.⁸³
-  4 A customer conducts 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. Indicators of possible front companies include opaque ownership structures, individuals and/or entities with obscure names that direct the company, or business addresses that are residential or co-located with other companies.

81. See Oct. 2018 FinCEN Advisory, *supra* note 1.

82. See Oct. 2023 FinCEN Alert, *supra* note 33.

83. As of February 2024, the Financial Action Task Force (FATF) has placed 21 jurisdictions on its Jurisdictions under Increased Monitoring or "Grey List" due to deficiencies in their anti-money laundering, terrorist financing, and proliferation financing regimes. See FATF, "[Jurisdictions under Increased Monitoring—23 February 2024](#)" (Feb. 23, 2024). In addition, the FATF defines Iran, the Democratic Republic of Korea, and Myanmar as "high-risk jurisdictions" due to significant strategic deficiencies in their anti-money laundering, terrorist financing, and proliferation financing regimes. See FATF, "[High-Risk Jurisdictions subject to a Call to Action—February 2023](#)" (Feb. 23, 2024).

-  A customer that is or purports to be a charitable organization or NPO⁸⁴ solicits donations but does not appear to provide any charitable services or openly supports terrorist activity or operations. In some cases, these organizations may post on social media platforms or encrypted messaging apps to solicit donations, including in CVC.
-  A customer receives numerous small CVC payments from many wallets, then transfers the funds to another wallet, particularly if the customer logs in using an Internet Protocol (IP) based in a jurisdiction known for, or at high risk for, terrorist activity. In such cases, financial institutions may also be able to provide associated technical details such as IP addresses with time stamps and device identifiers that can provide helpful information to authorities.
-  A customer makes money transfers to a jurisdiction known for, or at high risk for, terrorist activity that are inconsistent with their stated occupation or business purpose with vague stated purposes such as “travel expenses,” “charity,” “aid,” or “gifts.”
-  A customer account receives large payouts from social media fundraisers or crowdfunding platforms and is then accessed from an IP address in a jurisdiction known for, or at high risk for, terrorist activity, particularly if the social media accounts that contribute to the fundraisers contain content supportive of terrorist campaigns.
-  A customer company is incorporated in the United States or a third-country jurisdiction, but its activities occur solely in jurisdictions known for, or at high risk for, terrorist activity and show no relationship to the company’s stated business purpose.

84. FinCEN continues to emphasize that legitimate charities should have access to financial services and can transmit funds through legitimate and transparent channels. As set out in the Joint Fact Sheet on BSA Due Diligence Requirements for Charities and Non-Profit Organizations, banks are reminded to apply a risk-based approach to CDD requirements when developing the risk profiles of charities and other non-profit customers. The application of a risk-based approach is consistent with existing CDD and other Bank Secrecy Act/ AML compliance requirements. FinCEN, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency, [“Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations”](#) (Nov. 19, 2020).

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting Other Relevant BSA Reporting

USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

A financial institution is required to file a suspicious activity report (SAR) if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.⁸⁵ All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.⁸⁶

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, financial institution must also immediately notify, by telephone, an appropriate law enforcement authority and its regulator, in addition to filing a timely SAR.⁸⁷ Valuable cyber indicators for terrorist finance-related law enforcement investigations can include relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, virtual currency addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), and descriptions and timing of suspicious electronic communications.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.⁸⁸ Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.⁸⁹ When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

85. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.

86. See 31 U.S.C. § 5318(g)(3).

87. See, e.g., 31 CFR § 1020.320(b)(3) (Bank SAR rule). The other FinCEN SAR rules contain comparable provisions. See *id.*

88. See 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(c), 1030.320(c).

89. *Id.*; see also FinCEN, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

SAR Filing Instructions

FinCEN requests that financial institutions indicate any connection between the suspicious activity being reported and the activities highlighted in this advisory by including the key term “**IRANTF-2024-A001**” in SAR field 2 (“Filing Institution Note to FinCEN”), as well as in the narrative.

Financial institutions should select SAR Field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization) as the associated suspicious activity type. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

Financial institutions should include all available information relating to the account(s) and location(s) involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.⁹⁰

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).⁹¹

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting obligations to provide information in connection with the subject of this advisory. These include obligations related to the CTR,⁹² Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),⁹³ Report of Foreign Bank and Financial Accounts (FBAR),⁹⁴ Report of International Transportation of Currency or Monetary Instruments (CMIR),⁹⁵ Registration of Money Services Business (RMSB),⁹⁶ and Designation of Exempt Person (DOEP).⁹⁷ These standard reporting

90. See 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).

91. 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.

92. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than \$10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. See 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, 1026.310-313.

93. A report filed by a non-financial trade or business that receives currency in excess of \$10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. See 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.

94. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding \$10,000 at any time during the calendar year. See 31 CFR § 1010.350; FinCEN Form 114.

95. A form filed to report the transportation of more than \$10,000 in currency or other monetary instruments into or out of the United States. See 31 CFR § 1010.340.

96. A form filed to register an MSB with FinCEN, or to renew such a registration. See 31 CFR § 1022.380.

97. A report filed by banks to exempt certain customers from currency transaction reporting requirements. See 31 CFR § 1020.315.

requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this advisory, FinCEN requests that the filer select **Box 1b** (“suspicious transaction”) and include the key term “**IRANTF-2024-A001**” in the “**Comments**” section of the report.

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.⁹⁸ Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.⁹⁹ Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.¹⁰⁰ Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.¹⁰¹

98. See 31 CFR §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).

99. See 31 CFR §§ 1010.230, 1010.605(e)(1) (defining “covered financial institution”).

100. See 31 CFR § 1010.620. The definition of “covered financial institution” is found in 31 CFR § 1010.605(e)(1). The definition of “private banking account” is found in 31 CFR § 1010.605(m). The definition of “non-U.S. person” is found in 31 CFR § 1010.605(h).

101. See 31 CFR § 1010.620(c).

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,¹⁰² and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.¹⁰³ As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.¹⁰⁴

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing terrorist financing. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.¹⁰⁵ In accordance with the requirements of section 314(b) and its implementing regulations, FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with Foreign Terrorist Organizations (FTOs)¹⁰⁶ and Specially Designated Global Terrorists (SDGTs).¹⁰⁷

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

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

102. See 31 CFR §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.

103. See 31 CFR § 1010.610.

104. See FinCEN, [Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties](#), Interpretive Release 2004-1, 69 Fed. Reg. 74,439 (Dec. 14, 2004). See also FinCEN, [“Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring”](#) (Mar. 11, 2016).

105. See 31 CFR § 1010.540; see also, FinCEN, [“Section 314\(b\) Fact Sheet”](#) (Dec. 2020).

106. See Department of State, [“Foreign Terrorist Organizations.”](#)

107. Executive Office of the President, [“Executive Order 13224”](#) (Sep. 23, 2001).