



FinCEN ADVISORY

FIN-2025-A001

April 1, 2025

FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Advisory by including the key term “**ISIS-2025-A001**” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization).

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist financial institutions in identifying and reporting suspicious activity related to the financing of the Islamic State of Iraq and Syria (ISIS).¹ ISIS is a Sunni terrorist organization that has conducted and inspired terrorist attacks worldwide for more than a decade, killing or injuring thousands of people.² The U.S. Department of the Treasury’s (Treasury) 2024 National Terrorist Financing Risk Assessment notes that ISIS, which separated from al-Qa’ida (AQ) and declared itself a caliphate in 2014, remains a regional and global threat.³ While elements of ISIS’ central leadership remain in parts of Iraq and Syria where ISIS previously

controlled large swaths of territory,⁴ the group has numerous affiliates operating around the world, particularly in Africa, the Middle East, and Central Asia.⁵ Last year’s mass casualty attacks in Iran and Moscow by ISIS’s’ branch in Central Asia, known as ISIS-Khorasan (ISIS-K),⁶ as well as the 2025 New Year’s Day attack in New Orleans, carried out by an ISIS-inspired homegrown violent extremist

1. ISIS’s predecessor, Al-Qaeda in Iraq (AQI), was designated as a Foreign Terrorist Organization (FTO) in December 2004 in accordance with section 219 of the Immigration Nationality Act (INA), as amended, and this designation remains in effect for ISIS and many of its global affiliates. ISIS and its affiliates are also designated as Specially Designated Global Terrorists (SDGTs), pursuant to Executive Order (E.O.) 13224, as amended. For more information, *see* Office of the Director of National Intelligence (ODNI) National Counterterrorism Center (NCTC), “[Counter Terrorism Guide: Islamic State of Iraq and Ash-Sham \(ISIS\)](#)” (“Sept. 2022 Counter Terrorism Guide”) (Sept. 2022); and U.S. Department of State (State), “[Individuals and Entities Designated by the State Department Under Executive Order 13224](#).” The organization is sometimes referred to as the Islamic State of Iraq and ash-Sham (ISIS), the Islamic State of Iraq and the Levant (ISIL), and by its Arabic name, Da’esh.
2. *See* Sept. 2022 Counter Terrorism Guide, *supra* note 1.
3. *See* Treasury, “[2024 National Terrorist Financing Risk Assessment](#),” (“Feb. 2024 NTFRA”) (Feb. 2024), at p. 7; *see also* Sept. 2022 Counter Terrorism Guide, *supra* note 1; *see also* ODNI “[Annual Threat Assessment of the U.S. Intelligence Community](#)” (Feb. 5, 2024), at p. 38.
4. According to the ODNI’s 2025 Annual Threat Assessment, ISIS will seek to exploit the end of the Asad regime in Syria to reconstitute its attack capability, including external plotting, and to free ISIS prisoners to rebuild their ranks. *See* ODNI “[Annual Threat Assessment of the U.S. Intelligence Community](#)” (Mar. 2025), at pp. 6, 23.
5. *See* Congressional Research Service (CRS), “[The Islamic State: Background, Current Status, and U.S. Policy](#)” (“May 2024 CRS Background”) (May 6, 2024), at p. 1.
6. *Id.* at p.1. More recently, a member of ISIS-K was charged in the Aug. 2021 bombing at Hamid Karzai International Airport in Kabul which killed 13 American service members in addition to Afghan citizens during the U.S. troop withdrawal from Afghanistan. *See* U.S. Department of Justice (DOJ), “[United States Arrests ISIS-K Attack Planner for Role in Killing of U.S. Military Service Members at Abbey Gate, Afghanistan](#)” (March 5, 2025). For more information about ISIS-K, *see* DNI NCTC, “[ISIS Khorasan](#)” (As of Mar. 2025).

(HVE),⁷ demonstrate that the ISIS threat and influence remains far-reaching and that vigilance is required at home and abroad.

This Advisory is a continuation of the sustained effort that Treasury has led for more than a decade, in coordination with the U.S. government interagency and foreign partners, to disrupt and eliminate ISIS's revenue sources and financial networks.⁸ This Advisory is also consistent with the National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Priorities, which include terrorist financing, as well as Treasury's 2024 National Terrorist Financing Risk Assessment.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.

Overview

At the height of its influence in 2015, ISIS controlled large areas of Iraq and Syria, from which it launched attacks in the region and beyond.¹⁰ In addition, more than 42,000 foreign terrorist fighters (FTFs) from 120 countries traveled to Iraq and Syria between 2011 and 2016 to fight for ISIS.¹¹ During that time, ISIS organized and carried out mass-casualty attacks in Europe and the Middle East, notably the 2015 Paris attacks,¹² and inspired HVE attacks in the U.S. homeland, including the attacks in San Bernardino, California in 2015 and in Orlando, Florida in 2016.¹³ ISIS also engaged in acts of genocide, crimes against humanity, and ethnic cleansing against Yezidis, Christians, Shi'a Muslims, and in some cases, against Sunni Muslims, Kurds, and other minority groups in areas it controlled.¹⁴ ISIS was notorious for taking hostages of various nationalities, including American citizens located in the region, and demanding ransom payments in exchange for their release. While in ISIS captivity, these hostages were subjected to physical and psychological torture, and some were ultimately beheaded on video or killed through other means.¹⁵ These atrocities provided fuel for the ISIS propaganda machine: a

7. See Federal Bureau of Investigation (FBI), ["FBI Statement on the Attack in New Orleans"](#) ("Jan. 2025 FBI Statement") (Jan. 1, 2025), and [FBI Releases Investigative Update in Bourbon Street Attack](#) (Jan. 14, 2025).
8. See, e.g., Treasury, ["Counter ISIS Finance Group Leaders Issue Joint Statement"](#) (Aug. 8, 2024); ["Remarks by Assistant Secretary for Terrorist Financing Daniel Glaser at Chatham House"](#) (Feb. 8, 2016); ["Remarks by Counselor to the Secretary Carter Burwell at the Washington Institute"](#) (Dec. 15, 2020); and ["Treasury Targets ISIS Facilitation Network in Eastern, Central, and Southern Africa"](#) (Jul. 23, 2024).
9. FinCEN, ["Anti-Money Laundering and Countering the Financing of Terrorism National Priorities"](#) (June 30, 2021); see also Feb. 2024 NTFRA, *supra* note 3.
10. See May 2024 CRS Background, *supra* note 5, at p. 1.
11. United Nations Security Council (UNSC) Counter Terrorism Committee Executive Directorate, ["Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity, 2014-2024"](#) ("Nov. 2024 UNSC FTF Report") (Nov. 2024), at p. 5.
12. See CRS, ["The Islamic State and U.S. Policy"](#) ("Dec. 2015 CRS Report") (Dec. 8, 2015), at Summary.
13. 14 individuals were killed and 22 injured in the 2015 San Bernardino attack, while 49 individuals were killed and 53 others injured in Orlando. See U.S. Department of Homeland Security (DHS), ["Reference Aid: ISIS and al-Qa'ida-Inspired Homegrown Violent Extremists"](#) (Sept. 2017).
14. See State, ["Global Criminal Justice Regional Engagement"](#); ["10th Anniversary of ISIS's Genocide Against Yezidis, Christians, and Shi'a Muslims"](#) (Aug. 3, 2024).
15. See DOJ, ["ISIS 'Beagle' Sentenced to Life Imprisonment for Hostage-Taking Scheme that Resulted in the Deaths of American, British, and Japanese Citizens"](#) (Aug. 19, 2022). See also Wall Street Journal Video, ["Kayla Mueller, American Aid Worker, Killed While Held by ISIS"](#) (Feb. 10, 2015); U.S. Central Command, ["Statement from General Austin of Murder of Jordanian Pilot"](#) (Feb. 3, 2015).

sophisticated blend of traditional media platforms, glossy photos, in-depth articles, and social media campaigns used by the organization to drum up financial support and recruit fighters to join the cause.¹⁶

In 2019, following several years of sustained operations, a U.S.-led military coalition, in partnership with local forces, liberated the territory under ISIS's control in Iraq and Syria. This forced ISIS's activities in the region to become more clandestine. While it continued to carry out attacks, particularly against government and government-associated civilian targets, those attacks were smaller in scale and resulted in fewer casualties.¹⁷ Following the collapse of the caliphate, ISIS fighters, including FTFs and associates, were placed in detention facilities and open-air camps guarded by the U.S.-backed Syrian Democratic Forces. As of 2023, about 9,000 ISIS fighters remained in detention facilities, which are frequent targets for ISIS attacks,¹⁸ and as of 2024, approximately 43,000 people with links to ISIS remained in open air Al-Hol camp, most of whom are women and children.¹⁹ ISIS has sought to extend its influence into these camps and recruit among its residents, especially adolescents and third-country nationals. ISIS has also smuggled weapons, materials, money, and people into and out of the camps, strengthening the ties to ISIS cells outside the camps and making violence inside the camps more likely.²⁰

Counterterrorism efforts also led ISIS to become much more decentralized, operating in smaller, more autonomous cells, or affiliates, throughout the world.²¹ These affiliates receive operational guidance and funding from ISIS's General Directorate of Provinces' four regional offices.²² In Africa, ISIS has affiliates in Somalia, Libya, West Africa, the Sahel,²³ the Democratic Republic of the Congo, and Mozambique.²⁴ It also maintains a presence in Central,²⁵ South,²⁶ and Southeast Asia.²⁷ These affiliates vary in their goals, tactics, leadership structures, and threat profiles.²⁸ ISIS continues to

16. FBI, "[ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media](#)" (Jul. 6, 2016).
17. State, "[Iraq - Country Reports on Terrorism](#)" (2019).
18. See May 2024 CRS Background, *supra* note 5, at p. 1.
19. See DOD, "[Lead Inspector General Report to the United States Congress: Operation Inherent Resolve and Other U.S. Government Activities Related to Iraq & Syria](#)" (May. 02, 2024), at p. 30.
20. See DOD, "[Lead Inspector General Report to the United States Congress: Operation Inherent Resolve and Other U.S. Government Activities Related to Iraq & Syria](#)" (Sept. 30, 2023), at p. 33.
21. See ODNI "[Remarks by Acting Director of the National Counterterrorism Center at Center for Strategic and International Studies](#)" (Nov. 12, 2024).
22. The al-Furqan Office is responsible for West Africa and the Sahel; the Dhu al-Nurayn Office oversees North Africa and Sudan; al-Karrar Office covers East, Central, and Southern Africa, and Yemen regions; and Afghanistan-based al-Siddiq Office is responsible for South, Central and Southeast Asia. See Treasury, "[Fact Sheet: Countering ISIS Financing](#)" ("Jun. 2023 Treasury Fact Sheet") (Jun. 16, 2023), at p. 1.
23. The Sahel refers to the geographic region south of the Sahara desert that stretches from the Atlantic to Sudan, encompassing Mali, Mauritania, Chad, Niger, Burkina Faso, and parts of Nigeria.
24. See May 2024 CRS Background, *supra* note 5, at pp. 1-2. See also ODNI 2025 Annual Threat Assessment, *supra* note 4, at p. 6.
25. ISIS-K was established in Afghanistan in 2015 by Pakistani, Afghan, and Central Asian militants and has accelerated attacks in Afghanistan since the Taliban's return to power in 2021. See May 2024 CRS Background, *supra* note 5, at p. 1; see also Feb. 2024 NTFRA, *supra* note 3, at p. 7.
26. See, e.g., Treasury, "[Treasury Designates Leaders and Financial Facilitators of ISIS and al-Qa'ida Cells in Maldives](#)" ("Jul. 2023 Treasury Maldives Press Release") (Jul. 31, 2023).
27. See, e.g., UNSC, "[Islamic State in Iraq and the Levant in Southeast Asia \(ISIL-SEA, ISIL-South East Asia\)](#)" (Accessed Jun. 6, 2024).
28. See State, "[Terrorist Designation of ISIS General Directorate of Provinces Leaders](#)" (Jun. 8, 2023); See also May 2024 CRS Background, *supra* note 5, at p. 1.

attract FTFs, but recruitment efforts have become much more regional, reflective of the organization's broader trend towards regional autonomy and decentralization.²⁹ Despite this decentralization, however, ISIS's affiliates remain part of a network, with better-resourced branches financially supporting and subsidizing the activities of less affluent offshoots.³⁰

In addition, ISIS continues to inspire attacks by HVEs who do not receive individualized direction or have a formal affiliation with the organization but have been inspired to conduct violence, at least in part, by the group's ideology. The 2025 New Year's Day attack in New Orleans provides a recent example. The alleged perpetrator, Shamsud-Din Jabbar, was a U.S. citizen from Texas and had no known direct affiliation with ISIS but nevertheless drove a car bearing the ISIS flag into a crowd and then opened fire on law enforcement personnel after expressing support for the organization.³¹

Raising Funds

When it controlled territory in Iraq and Syria, ISIS was able to fund itself and its affiliates by exploiting oil and other natural resources, taxing and extorting local populations, kidnapping for ransom, and selling looted antiquities.³² ISIS's access to natural resources was cut off in Iraq and Syria after it lost territory in 2019, and its ability to tax and extort local populations was diminished, though not eliminated. As a result, ISIS organizational funds have dwindled to \$10-20 million, mostly held cash and other liquid assets.³³ Today, ISIS in Iraq and Syria and its global affiliates fund themselves through a combination of taxation and extortion of local populations and businesses, resource extraction, kidnapping for ransom, crowdfunding, and donations, depending on the region.³⁴

Taxation and Extortion

Most of ISIS's affiliates around the world, including ISIS in Iraq and Syria, rely to some extent on extortion of local businesses as a source of revenue.³⁵ ISIS-Somalia has been successful in extorting local businesses. For example, in the first half of 2022 alone, ISIS-Somalia raised \$2 million from extortion payments from local businesses, imports, livestock, and agriculture.³⁶ In West Africa, ISIS has established a proto-state that relies upon the enforcement of religious taxes for funding.³⁷ Extortion is also a key funding mechanism for ISIS-K in Central Asia.³⁸

29. See Nov. 2024 UNSC FTF Report, *supra* note 11, at pp. 4, 6.

30. See Feb. 2024 NTFRA, *supra* note 3, at p. 8. See also May 2024 CRS Background, *supra* note 5, at p. 2.

31. See FBI, "[Investigative Updates on the New Orleans Bourbon Street Attack](#)" (Jan. 2, 2025).

32. See Dec. 2015 CRS Report, *supra* note 12, at p. 28.

33. Treasury further assesses that from January to December 2024, ISIS probably generated around \$8 million through activities such as kidnapping for ransom, extortion, zakat (or taxation) and through donations from international supporters. See Treasury, "[Fact Sheet: Countering ISIS Financing](#)" ("Feb. 2024 Treasury Fact Sheet") (Feb. 27, 2024), at p. 1.

34. *Id.* at p. 2.

35. Treasury, "[Fact Sheet on ISIS Financing](#)" ("Aug. 2024 Treasury Fact Sheet") (Aug. 8, 2024), at p. 1.

36. Treasury, "[Treasury Designates Senior ISIS-Somalia Financier](#)" (Jul. 27, 2023).

37. See Feb. 2024 Treasury Fact Sheet, *supra* note 33, at p. 2.

38. See Aug. 2024 Treasury Fact Sheet, *supra* note 35, at p. 2.

Resource Extraction and the Spoils of War

In cases where ISIS affiliates exert control over territory, they sometimes generate revenue through the extraction and sale of natural resources. The ISIS affiliate in the Democratic Republic of the Congo (ISIS-DRC), for example, supplements its funding from ISIS leadership by taxing illegal gold mines and smugglers, as well as by operating artisanal mining projects.³⁹ More often, however, ISIS affiliates fund themselves through the “spoils of war,” or goods and resources plundered from local communities. ISIS-Sahel is particularly reliant on the spoils of war and could possibly generate as much as \$6 million per year by some estimates, but this is not a stable or consistent source of income.⁴⁰

Kidnapping for Ransom

The ISIS caliphate became notorious in the late 2010s for generating revenue through kidnapping for ransom. Many of ISIS’ global affiliates continue to use this tactic today. Targets of these kidnappings have included local government personnel, foreign aid workers, journalists, Christians, and other civilians whom ISIS perceives to be working against the group or opposed to its interpretation of Islamic law.⁴¹ In other cases, the group abducts ordinary civilians to inspire fear in local populations.⁴² Kidnapping for ransom generates a significant amount of revenue for ISIS-K in Central Asia,⁴³ and ISIS branches in Mozambique, the Sahel, West Africa, and North Africa have also profited by kidnapping and ransoming foreign nationals.⁴⁴

Crowdfunding and Donations

ISIS frequently solicits donations through its official websites and publications, and on social media platforms, and has received financial support from sympathizers around the world. ISIS-K, for example, has frequently published posters in its flagship magazine, the Voice of Khorasan, that contain QR codes that enable supporters to send donations using virtual currency.⁴⁵ These campaigns employ diverse techniques to collect and launder virtual currency, including addresses shared among campaign members, rapid fund transfers between largely unhosted addresses, temporary addresses, cross-blockchain movement, asset conversion, and various systems for converting virtual currencies into cash.⁴⁶

39. *Id.* at p. 2.

40. *Id.* at p. 2.

41. See DNI NCTC, “[ISIS -- West Africa](#)” (Sept. 2022); and State, “[Country Reports on Terrorism 2022](#)” (2022).

42. See State, “[Country Reports on Terrorism - Cameroon](#)” (2022), “[Country Reports on Terrorism - Nigeria](#)” (2022), “[Country Reports on Terrorism - Mozambique](#)” (2022).

43. See Feb. 2024 Treasury Fact Sheet, *supra* note 33, at p. 2.

44. See Aug. 2024 Treasury Fact Sheet, *supra* note 35, at p. 2. See also Jun. 2023 Treasury Fact Sheet, *supra* note 22, at pp. 1-2.

45. *Id.* at p. 2.

46. See Nov. 2024 UNSC FTF Report, *supra* note 11, at p. 13.

Individuals have also taken it upon themselves to raise funds for ISIS, coordinating donation drives through encrypted mobile applications.⁴⁷ Donations from supporters are usually derived from legal sources, such as personal savings,⁴⁸ but they have also been generated by illicit means such as fraudulently obtaining large numbers of loans or credit cards.⁴⁹ Contributions are collected in a centralized bank account, peer-to-peer (P2P) platform account, or digital asset wallet either belonging to the coordinator of the fundraiser or to a nominee, usually a friend or family member. Once amassed, the funds may be sent to ISIS members in the form of digital assets, wired abroad through a fiat MSB, or withdrawn in cash and passed to couriers who deliver the money to ISIS members abroad.⁵⁰

Fraudulent Humanitarian Appeals

ISIS supporters sometimes disguise fundraising campaigns as humanitarian relief efforts, taking advantage of relief efforts for natural disasters or conflicts in regions where ISIS is prevalent to divert humanitarian assistance.⁵¹ To do this, ISIS mimics the fundraising campaigns of non-profit organizations (NPOs), but these fraudulent charitable appeals are most commonly made without the involvement of a registered NPO. This method allows groups to cast a wide net to raise funds online, either through social media or dedicated crowdfunding websites.⁵²

ISIS supporters also frequently initiate fundraisers to benefit displaced persons in the al-Hol and Roj camps in northeastern Syria.⁵³ These fundraising campaigns generally avoid expressing overt support for ISIS but use specific religious terminology and imagery to signal affiliation with the group. Campaigns are primarily promoted in Arabic and English, but have appeared in other languages such as Russian, German, and French.⁵⁴ ISIS sympathizers in over 40 countries have sent money to ISIS-linked individuals in these camps.⁵⁵ Funds generated from these campaigns typically make their way to the camps in Syria via cash couriers or the hawala system.⁵⁶

47. See Feb. 2024 NTFRA, *supra* note 3, at p. 9. See, e.g., DOJ, [“Four Defendants Charged with Conspiring to Provide Cryptocurrency to ISIS”](#) (“Dec. 2022 DOJ Press Release”) (Dec. 14, 2022); [“Tajik National Arrested in Brooklyn for Conspiring to Provide Material Support to ISIS”](#) (Feb. 26, 2025).

48. See Dec. 2022 DOJ Press Release, *supra* note 47.

49. See DOJ, [“Long Island Woman Sentenced to 13 Years’ Imprisonment for Providing Material Support to ISIS”](#) (Mar. 13, 2020).

50. See Feb. 2024 NTFRA, *supra* note 3, at p. 9.

51. See, e.g., Treasury, [“Counter ISIS Finance Group Leaders Issue Joint Statement”](#) (Feb. 27, 2024).

52. See Feb. 2024 NTFRA, *supra* note 3, at p. 25.

53. Al-Hol is an internally displaced person’s camp in northern Syria. It holds one of the largest concentrations of current and former ISIS members who continue to receive donations from ISIS supporters internationally. See Treasury, [“Overseas Contingency Operations - Summary of Work Performed by the Department of the Treasury Related to Terrorist Financing and Anti-Money Laundering for the First Quarter Fiscal Year 2025”](#) (Feb. 27, 2025).

54. See Nov. 2024 UNSC FTF Report, *supra* note 11, at p. 13.

55. Treasury, [“Treasury Designates Facilitation Network Supporting ISIS Members in Syria”](#) (“May 2022 Treasury Press Release”) (May 9, 2022).

56. In July 2020, Treasury designated Faruq Hamud, who had been operating as a hawaladar within the al-Hol camp offering his services to ISIS members. See Treasury, [“Treasury Designates Key ISIS Financial Facilitators in the Middle East”](#) (“Jul. 2023 Treasury Somalia Press Release”) (Jul. 28, 2020).

Moving Funds

While each ISIS affiliate has its own methods of generating revenue locally, larger affiliates sometimes distribute funds to other ISIS affiliates.⁵⁷ ISIS-Somalia has facilitated funds transfers to other branches and networks through mobile money platforms, cash transfers, hawalas,⁵⁸ and money laundering through businesses.⁵⁹ In the past, ISIS-K, has been financed from ISIS's organizational funds to carry out attacks.⁶⁰ To move these funds internationally, ISIS still frequently uses cash couriers; however, it also uses banks and money service businesses (MSBs), especially hawalas, unregistered money transmitters, and digital assets exchanges.⁶¹

Banks, Hawalas, and other MSBs

In some cases, ISIS directly leverages the regulated financial system to move money internationally, taking advantage of jurisdictions with weak AML/CFT controls to launder funds. For example, ISIS-Somalia has used banks to launder funds, and bank accounts in South Africa have been utilized to transfer funds to ISIS in Central Africa.⁶²

ISIS relies much more heavily, however, on both registered and unlicensed MSBs, especially hawalas.⁶³ Treasury has sanctioned several hawala operators and MSBs in Africa and the Middle East, often owned and operated by ISIS members, that have played key roles in moving funds internationally on behalf of the organization.⁶⁴ These hawala operators serve as key hubs in ISIS's international financial facilitation networks stretching from the Middle East to South Asia.⁶⁵ These international networks also facilitate weapons trafficking and human smuggling for the organization.⁶⁶ Hawalas are also a key way in which funds make their way to ISIS members in the

57. See Feb. 2024 NTFRA, *supra* note 3, at p. 8.

58. The Financial Action Task Force (FATF) defines hawalas and other similar service providers (HOSSPs) as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. See FATF, "[The Role of Hawala and Other Similar Service Providers in ML/TF](#)" ("Oct. 2013 FATF Hawala Report") (Oct. 2013), at p. 9.

59. See Feb. 2024 NTFRA, *supra* note 3, at p. 8; see also May 2024 CRS Background, *supra* note 5, at p. 2. On Feb. 1, 2025, ISIS-Somalia was targeted in the Golis mountains in airstrikes coordinated with the Federal Government of Somalia. See DOD, "[Secretary of Defense Pete Hegseth Statement on U.S. Africa Command Strikes in Somalia](#)" (Feb. 1, 2025).

60. See Aug. 2024 Treasury Fact Sheet, *supra* note 35, at p. 1, and note 6.

61. See Feb. 2024 NTFRA, *supra* note 3, at p. 8.

62. See Feb. 2024 Treasury Fact Sheet, *supra* note 33, at pp. 1-2.

63. See note 58 for a definition of hawala. Depending on how they operate, hawalas can be either registered or unlicensed MSBs. There is no practical or functional distinction between a hawala and any other money transmitter. While it is theoretically possible for informal value transfer systems (IVTS) to operate wholly outside the banking system, it is not often the case. Instead, law enforcement investigations indicate IVTS often use account at banks to clear and settle transactions internationally. For more information, see Treasury, "[2024 National Money Laundering Risk Assessment](#)" (Feb. 2024), at p. 71.

64. See Treasury, "[Treasury Designates Key Nodes of ISIS's Financial Network Stretching Across the Middle East, Europe, and East Africa](#)" (Apr. 15, 2019); "[Counter ISIS Finance Group Leaders Issue Joint Statement](#)" (May 17, 2022); Jul. 2023 Treasury Somalia Press Release, *supra* note 56; and "[Treasury Sanctions South Africa-based ISIS Organizers and Financial Facilitators](#)" (Mar. 1, 2022).

65. See generally Treasury, "[The United States and Türkiye Take Joint Action to Disrupt ISIS Financing](#)" (Jan. 5, 2023).

66. In 2023, ISIS-K used Türkiye as a transit hub for disbursing funds and transferring operatives and weapons from Afghanistan to Europe for possible attacks. See Feb. 2024 NTFRA, *supra* note 3, at p. 8. See also Treasury, "[Treasury Targets ISIS-linked Human Smuggling Network in Coordinated Action with Türkiye](#)" (June 14, 2024).

displaced persons camps in Northern Syria, where they are used to free ISIS sympathizers and recruit on behalf of the organization.⁶⁷ In al-Hol camp alone, ISIS supporters have received up to \$20,000 per month via hawalas, with the majority of those funds transfers originating outside Syria or passing through neighboring countries such as Türkiye.⁶⁸

ISIS also makes use of online payment providers, including some social media companies, to move funds. Some of these online payment providers operate as unregistered MSBs in the United States. The organization also makes use of MSBs that have incorporated digital assets into their business models, many of which also operate as unregistered MSBs.⁶⁹

Digital Assets

ISIS and its affiliates have increasingly adopted digital assets, including virtual currency, as a means of storing and moving funds.⁷⁰ In 2023, the United Nations reported that ISIS's Al-Karrar office sent up to \$25,000 to ISIS-K in virtual currency each month.⁷¹ Furthermore, as part of the 2024 Crocus Hall attack in Moscow, ISIS-K reportedly transferred at least \$2,000 in virtual currency to the attackers.⁷²

ISIS is reported to have used Bitcoin as well as stablecoins like Tether (USDT) to raise and move funds but has also promoted fundraising campaigns using the blockchains Ethereum, Monero, and Tron.⁷³ Virtual assets have been sent directly to ISIS supporters located in northern Syria, often to Idlib, or indirectly via Türkiye, where ISIS is able to access them through virtual asset trading platforms.⁷⁴ To this end, ISIS takes advantage of virtual currency exchanges with lax or non-existent AML/CFT controls to send, receive, and convert these funds.⁷⁵

67. See also Feb. 2024 NTFRA, *supra* note 3, at p. 8.

68. See May 2022 Treasury Press Release, *supra* note 55.

69. See Feb. 2024 NTFRA, *supra* note 3, at pp. 8, 17.

70. See Aug. 2024 Treasury Fact Sheet, *supra* note 35, at p. 2. The term “virtual currency” refers to a medium of exchange that can operate like currency, but does not have all the attributes of “real” currency, including legal tender status. See FinCEN, [“Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,”](#) (May 9, 2019).

71. UNSC, [“Thirty-first report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 \(2021\) concerning ISIL \(Da’esh\), Al-Qaida and associated individuals and entities”](#) (“Feb. 2023 UNSC Report”) (Feb. 13, 2023), at p. 8.

72. See Aug. 2024 Treasury Fact Sheet, *supra* note 35, at p. 2.

73. Stablecoins are virtual assets that are designed to maintain a stable value relative to a national currency or other reference assets. See Feb. 2024 NTFRA, *supra* note 3, at p. 20.

74. See Treasury, [“Action Plan to Address Illicit Financing Risks of Digital Assets”](#) (Sep. 20, 2022), at p. 4.

75. For example, in 2023, virtual currency exchange Binance settled with FinCEN and OFAC for willful violations of the BSA and apparent violations of multiple sanctions programs. The violations include failure to implement an AML program and failure to file suspicious activity reports on terrorists, including ISIS. 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). At the same time, Binance pleaded guilty to three criminal charges: conspiracy to conduct an unlicensed money transmitting business and failure to maintain an effective anti-money laundering program, conducting an unlicensed money transmitting business, and violating U.S. sanctions. See DOJ, [“Binance and CEO Plead Guilty to Federal Charges in \\$4B Resolution”](#) (Nov. 21, 2023).

Case Study

Virginia Man Convicted for Crypto Financing Scheme to ISIS

A jury convicted Mohammed Azharuddin Chhipa, 35, of Springfield, Virginia, on Dec. 13, 2024, for charges relating to his efforts to provide material support to ISIS.

According to court records and evidence presented at trial, from at least October 2019 through October 2022, Chhipa collected and sent money to female ISIS members in Syria to benefit ISIS in various ways, including by financing the escape of female ISIS members from prison camps and supporting ISIS fighters. Chhipa would raise funds online on various social media accounts. He would receive electronic transfers of funds and travel hundreds of miles to collect funds by hand. He would then convert the money to cryptocurrency and send it to Türkiye, where it was smuggled to ISIS members in Syria.

His primary co-conspirator was a British-born ISIS member residing in Syria who was involved in raising funds for prison escapes, terrorist attacks, and ISIS fighters. Over the course of the conspiracy, the defendant sent out over \$185,000 in cryptocurrency.⁷⁶

Homegrown Violent Extremism Inspired by ISIS

ISIS advocates through videos and other English language propaganda for supporters to conduct attacks in the United States and Western countries and has specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.⁷⁷ Actors who carry out these attacks are referred to as HVEs and are defined as individuals who live and operate in the United States and who advocate, are engaged in, or are preparing to engage in ideologically motivated terrorist activities inspired by foreign terrorist organizations (FTOs) like ISIS or their ideologies but who act independently of direction by an FTO.⁷⁸ Furthermore, according to DHS, ISIS online media groups have used the Israel-Hamas conflict to encourage attacks against the West and Jewish and Christian communities. ISIS media outlets have also capitalized on recent attacks in Europe in attempts to inspire more violent action.⁷⁹

Since 2015, HVEs have shown an interest in a wide range of targets, including law enforcement, U.S. military, and civilian targets. HVEs are most likely to use easy-to-acquire weapons such as firearms and edged weapons and will also occasionally use vehicles.⁸⁰ According to the FBI, attackers inspired

76. DOJ, "[Virginia Man Convicted for Crypto Financing Scheme to ISIS](#)" (Dec. 16, 2024).

77. DOJ, "[Statement of Christopher A. Wray Director Federal Bureau of Investigation before the Committee of the Judiciary United States Senate](#)" ("Dec. 2023 Statement of Christopher Wray") (Dec. 5, 2023), at p. 4.

78. In December 2023, the FBI assessed HVEs as the greatest, most immediate international terrorism threat to the homeland due to their lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications, which pose significant challenges to law enforcement's ability to proactively identify and disrupt potential violent attacks. See Dec. 2023 Statement of Christopher Wray, *supra* note 77, at pp. 2-3.

79. DHS, "[Homeland Threat Assessment 2025](#)" (2025), at p. 3.



80. DHS Countering Violent Extremism (CVE) Task Force, "[Reference Aid: ISIS and al-Qa'ida-Inspired Homegrown Violent Extremists](#)" ("Sept. 2017 DHS Reference Aid") (Sept. 2017), at p. 1.

by FTOs who have conducted vehicle attacks in the United States and abroad have used rented, stolen, and personally owned vehicles.⁸¹

HVE activities tend to be funded through legal means, like personal savings and the sale of personal assets.⁸² While there are limited financial indicators that are unique to HVE activity, some HVE attacks have been preceded by sudden account closures or disbursements, as well as the sudden urgent liquidation of valuable personal assets with no apparent concern for financial gain.⁸³ Analysis of BSA data relating to HVE activity also indicates that sudden inexplicable changes in activity, like the sudden adoption or increased use of financial methods that conceal the ultimate source or end use of funds—such as peer-to-peer (P2P) transfers, ATM withdrawals, third party payment processors, prepaid cards, and wire transfers—may also be an early indicator of HVE activity. Frequent unexplained cash deposits, especially if the individual is unemployed or if these deposits are in addition to a regular paycheck, may indicate that the individual is working with a wider network.⁸⁴ Analysis of BSA data relating to HVE activity also indicates that registered MSBs appear to be the preferred method of sending and receiving funds for domestic supporters of FTOs. These funds tend to be sent in low dollar amounts to avoid suspicion from financial institutions and law enforcement.

Red Flag Indicators Related to the Financing of ISIS and its Global Affiliates

FinCEN has identified the red flags listed below to assist financial institutions in detecting, preventing, and reporting suspicious activity connected to the financing of ISIS. 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.









-  One credit card or bank account is used to book travel to or accommodation and transportation in an area of known ISIS activity for several unrelated people at the same time for no known legitimate purpose.
-  Fundraisers are attached to social media profiles that show support for ISIS or display ISIS-related iconography or refer to supporting the “mujahideen” or the “war against kufar (non-believers),” especially if the fundraisers are soliciting donations to fund travel to an area of known ISIS activity. The fundraising appeal posted on social media references aid to imprisoned women and children in Iraq or Syria.

81. Internet Crime Complaint Center (IC3), [“Threat of Copycat Attacks after ISIS-Inspired Vehicle Attack in New Orleans”](#) (Jan. 13, 2025).

82. See Feb. 2024 NTFRA, *supra* note 3, at p. 9.

83. See for example, DOJ, [“Afghan National Arrested for Plotting an Election Day Terrorist Attack in the Name of ISIS”](#) (Oct. 8, 2024); see also DNI, [“US Violent Extremist Mobilization Indicators”](#) (“2021 DNI Mobilization Indicators”) (2021), at p. 11.

84. See 2021 DNI Mobilization Indicators, *supra* note 83, at p. 16.

-  A customer collects small amounts through P2P transfers, social media, or virtual currency payments over a short period of time and then sends them in a lump sum to an individual located in a region where ISIS presence is prevalent.
-  A customer sends remittances with no known legitimate purpose from the United States to multiple individuals in jurisdictions, such as Türkiye, known for ISIS facilitation activity who do not appear to have any relation to the sender.
-  A customer attempts to purchase plane or other travel tickets after abruptly liquidating assets, closing accounts, cancelling subscriptions, or receiving large unexplained sums of cash. A period of account dormancy following these behaviors should also be regarded as suspicious, even if the customer eventually resumes transactions within the United States.
-  A customer abruptly appears to seek as many lines of credit as possible, for example, by acquiring several credit cards and taking out one or more loans for unclear reasons, especially if the customer has not used credit cards or taken out loans in the past. This behavior should be regarded as especially suspicious if the customer uses newly obtained credit cards either exclusively or almost exclusively for cash advances and purchases of virtual currencies but then fails to make loan or credit card payments when they come due.
-  A customer begins receiving a sudden influx of unexplained cash deposits, especially if that customer is unemployed or these deposits are in addition to a regular paycheck, or if the deposits come from ATMs in locations where ISIS is prevalent, but where the customer is not known to reside or have traveled.
-  A customer suddenly adopts or increases their use of financial methods that conceal the ultimate source or end use of funds, for example P2P transfers, ATM withdrawals, third party processors, prepaid cards, virtual currency, or wire transfers.
-  A customer makes deposits in an account locally which are then withdrawn from other locations, including from abroad, where the individual is not known to reside or have traveled but where ISIS is prevalent.
-  A customer places virtual currency in a virtual currency wallet using an IP address in one location which is then withdrawn from virtual currency kiosks or converted to fiat currency by users with IP addresses in different locations where the individual is not known to reside or have traveled but where ISIS is prevalent.
-  A customer's account appears to have been accessed in multiple countries at the same time or within a very short time period, particularly if the account is accessed in countries where ISIS is prevalent.

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

*Suspicious Activity Reporting
Law Enforcement Filing Tips
Other Relevant BSA Reporting*

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

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.⁸⁷ 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.⁸⁸ 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.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping ISIS financing. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Advisory by including the key term "**ISIS-2025-A001**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory or notice keywords in the narrative, if applicable.

85. 31 U.S.C. § 5318(g)(1). *See also* 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). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

87. *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(d), 1030.320(d).

88. *Id.*; *see also* FinCEN, "[Suspicious Activity Report Supporting Documentation](#)" (June 13, 2007).

Financial institutions should select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization). Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR Fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the depositing or cashing of suspicious checks and the status of their accounts with the institution. 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.⁸⁹

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, a financial institution should also immediately notify, by telephone, an appropriate law enforcement authority, in addition to filing a timely SAR.⁹⁰ Immediate notification to law enforcement is especially important in situations involving suspected terrorist activity, as terrorists and terrorist organizations often rely on the international financial system to acquire funding to sustain and finance their operations and engage in acts of terrorism. Additionally, FinCEN emphasizes that any financial institution and any director, officer, employee, or agent of such institution who makes, or requires another to make any voluntary disclosure of any possible violation of law or regulation to a government agency under the BSA or its implementing regulations is protected from liability for any such disclosure.⁹¹

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).⁹²

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this Advisory. These include obligations related to the Currency Transaction Report (CTR),⁹³

89. 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).

90. See, e.g., 31 CFR §§ 1020.320(b)(3), 1022.320(b)(3), 1023.320(b)(3).

91. 31 U.S.C. 5318(g)(3); see, e.g., 31 CFR 1020.320(f).

92. 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.

93. 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, and 1026.310-313.

Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),⁹⁴ Report of Foreign Bank and Financial Accounts (FBAR),⁹⁵ Report of International Transportation of Currency or Monetary Instruments (CMIR),⁹⁶ Registration of Money Services Business (RMSB),⁹⁷ and Designation of Exempt Person (DOEP).⁹⁸

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.⁹⁹ Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.¹⁰⁰ 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.¹⁰¹ 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

94. A report filed by a 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 §§ 1010.330-331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.
95. 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.
96. 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.
97. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. *See* 31 CFR § 1022.380.
98. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 CFR § 1010.311.
99. *See* 31 CFR §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).
100. *See* 31 CFR §§ 1010.230, 1010.650(e)(1) (defining “covered financial institution”).
101. *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).

held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.¹⁰²

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,¹⁰³ 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.¹⁰⁴ 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.¹⁰⁵

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.¹⁰⁶ 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)¹⁰⁷ and Specially Designated Global Terrorists (SDGTs).¹⁰⁸

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 Advisory should be addressed to the FinCEN Regulatory Support Section at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit activity, 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.

102. See 31 CFR § 1010.620(c).

103. 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.

104. See 31 CFR § 1010.610.

105. 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).

106. See 31 CFR § 1010.540; see also, FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).

107. See Department of State, ["Foreign Terrorist Organizations."](#)

108. Executive Office of the President, ["Executive Order 13224"](#) (Sep. 23, 2001).