Department of the Treasury

2026 National Terrorist Financing Risk Assessment

March 2026

Department of the Treasury

2026 National Terrorist Financing Risk Assessment

CONTENTS

EXECUTIVE SUMMARY

Since the last National Terrorist Financing Risk Assessment (NTFRA) was published in 2024, the global security landscape has shifted—new threats have emerged and old ones have been reinvigorated, while major geopolitical events have shaped terrorism threats in unprecedented ways. The post-October 7, 2023, environment has proven to be a fertile breeding ground for terrorist radicalization and violent extremism, both on an individual and organizational level, as terrorist groups have called for increased violence and financial support. Additionally, the fall of the Assad regime in Syria has created instability that terrorist groups may seek to exploit for territorial expansion or fundraising.[1] These, along with other major geopolitical developments in Iran, Israel, Gaza, and Lebanon, have already reshaped terrorism threats—in some cases galvanizing new actors, and in other cases, degrading existing terrorist groups.

In addition to these unfolding complexities across the Middle East, the epicenter of global terrorism has increasingly shifted to Sub-Saharan Africa as affiliates of the Islamic State of Iraq and Syria (ISIS) and Al-Qa'ida (AQ), two designated foreign terrorist organizations (FTOs), have further established themselves there and waged lethal campaigns of violence across the continent. The past two years have also demonstrated that regardless of ideology, terrorist groups continue to show resilience in the face of military and financial pressure. This is particularly true for Iran-backed terrorist groups such as Harakat al-Muqawama al-Islamiya (Hamas) and Hizballah, the threat from which has not been significantly diminished despite both being degraded over the course of the Israel-Hamas war.

Against the backdrop of the ever-evolving terrorist threat landscape, the United States still faces a range of terrorist threats from an ideologically diverse array of actors. The 2025 ISIS-inspired New Years Day terrorist attack in New Orleans served as a stark reminder that the greatest terrorism threat the United States faces is from homegrown violent extremists (HVEs), inspired by FTOs, or similar ideology who are radicalized to violence online, and can aspire to commit lone offender attacks.[2] A series of other disrupted terrorist plots since New Orleans has further underscored this fact.[3] The individualized nature of the threat posed by HVEs makes it profoundly challenging for law enforcement (LE) to detect and disrupt the attacks before they occur. For these types of low-cost attacks, self-funding continues to be the predominant method of financial support, which can limit the ability of financial institutions to identify activity indicative of terrorist financing (TF) and proactively notify law enforcement. The United States also continues to face significant threats from individual extremists inspired by a range of domestic ideological and sociopolitical grievances, who commit lone, self-funded attacks or acts of violence on targets in the United States.

At the same time, other major threats to the U.S. homeland have necessitated using new tools. In January 2025, the Trump Administration took the unprecedented step of designating certain international drug cartels and transnational criminal organizations (TCOs) as FTOs and Specially Designated Global Terrorists (SDGTs) and adopted the policy of pursuing the total elimination of these organizations' presence in the United States. As of December 2025, the Administration has designated fifteen TCOs based in the Western Hemisphere as FTOs. These groups are sophisticated and well-organized, using violence to control neighborhoods and territory, and they finance themselves through various crimes, including drug trafficking, human trafficking and human smuggling, arms trafficking, robbery, timeshare fraud, oil and fuel smuggling, kidnapping, extortion, targeted killings, and

1 The E.O. of June 30, 2025, removed sanctions on Syria effective July 1, 2025 while maintaining sanctions on Bashar al-Assad and certain other destabilizing regional actors.

2 For example, Department of Justice, "Michigan Man Arrested and Charged with Attempting to Attack Military Base on Behalf of ISIS," (May 14, 2025), https://www.justice.gov/opa/pr/michigan-man-arrested-and-charged-attempting-attack-military-base-behalf-isis.

3 See, e.g., Department of Justice, "Pakistani National Extradited to Face Charges in Connection with Plot to Carry Out ISIS-Inspired Mass Shooting at Jewish Center in New York City," (Jun. 10, 2025), https://www.justice.gov/opa/pr/pakistani-national-extradited-face-charges-connection-plot-carry-out-isis-inspired-mass; Department of Justice, "Man Sentenced to Nine Years in Prison for Attempting to Provide Material Support to ISIS," (Sep. 23, 2025), https://www.justice.gov/opa/pr/man-sentenced-nine-years-prison-attempting-provide-material-support-isis.

other schemes. The FTO designations enable the United States to consolidate and maximize its sanctions tools, law enforcement efforts, and other resources against these violent drug cartels and transnational criminal organizations.[4] For the first time, the risks posed by TCOs will be discussed in the NTFRA in addition to the National Money Laundering Risk Assessment (NMLRA).

U.S. personnel, allies, and interests overseas remain at risk of terrorist attacks, particularly by ISIS or AQ affiliates and Iran-supported groups. Overall, ISIS and AQ remain the most lethal terrorist groups globally and still aspire to conduct or inspire attacks against the U.S. homeland. These FTOs continue to rely on historical methods of raising funds, exploiting whatever illicit revenue generating activities are available where they operate. While Hamas and Hizballah have been weakened over the past two years, they still pose a persistent threat to international security and the U.S. financial system. They continue to find ways to abuse the U.S. banking system, exploiting the reach and volume of U.S. dollar transactions throughout the world, and continue to receive large sums of money from Iran, the world's leading state sponsor of terrorism. All these groups continue to rely on key financial and logistics hubs in permissive jurisdictions to move funds.

Within the United States, there has been a continued pattern of domestic supporters sending funds abroad or fundraising on behalf of terrorist groups — most often ISIS. While digital assets (i.e., virtual currencies) are not the primary method that terrorist groups use to transfer funds abroad, they have become a popular choice for U.S.-based supporters to move funds, in addition to continued use of money services businesses (MSBs) and cash. Additionally, some domestic supporters of FTOs have continued to abuse various vulnerabilities within the U.S. financial system to fundraise online for terrorist groups. Increasingly, these individuals have taken measures to improve the operational security of their efforts to fundraise, such as by intentionally moving conversations to encrypted messaging platforms. Lastly, while there are fewer American foreign terrorist fighters (FTFs) traveling to combat zones than there were 10 years ago, FTFs are increasingly traveling to Africa—with similar self-financing methods as in years past—consistent with the shifting theaters of terrorism.

4 See further discussion on the financing of transnational criminal organizations (TCOs) and money laundering related to drug trafficking in the 2026 National Money Laundering Risk Assessment, p. 21-26.

INTRODUCTION

The 2026 NTFRA identifies the TF threats, vulnerabilities, and risks that the United States currently faces, updating the 2024 NTFRA. This report, as well as the 2026 NMLRA and 2026 National Proliferation Financing Risk Assessment (NPFRA), provide an overview of the current illicit finance risks to the United States.

Relevant component agencies, bureaus, and offices of the U.S. Department of the Treasury (Treasury), U.S. Department of Justice (DOJ), federal financial regulators, and other government agencies participated in developing the risk assessment. The 2026 NTFRA is based on an analysis of criminal prosecutions[5], consultations with relevant authorities and private sector entities, and a review of government actions and analysis, including Treasury designations and private sector research issued since the 2024 NTFRA.[6]

THREATS

The threats discussed below represent the terrorist groups and their supporters, including U.S.-based individuals and facilitators, who are most active in raising or moving funds through the United States or the U.S. financial system. While other terrorist threats pose harm to U.S. interests and personnel abroad, this assessment focuses on those threats that have a demonstrable nexus to the U.S. financial system. In 2026, the major TF threats to the United States include ISIS, AQ, Hamas, Hizballah, HVEs, and domestic violent extremists (DVEs).

Islamic State of Iraq and Syria (ISIS)

ISIS continues to pose a potent threat to stability and peace around the world both through direct actions by its affiliates and through franchising its violence by inspiring individual acts of terrorism. Despite continued counterterrorism pressure and the loss of a third ISIS leader in 2025, ISIS has continued to show its resiliency and still aspires to execute attacks on the West. It has sought to capitalize on the conflict in the Middle East to spread terrorist propaganda, recruit sympathizers, fundraise online, and call for increased attacks and violence. In 2024, ISIS-Khorasan (ISIS-K), one of the most operationally capable ISIS branches in central and south Asia, sustained a steady level of high profile, operationally complex, and lethal attacks outside its normal sphere of influence, including in Iran, Russia, Syria, and Oman, though this frequency has not kept pace in 2025. Additionally, ISIS's presence and influence in Iraq and Syria—which was significantly curtailed by the U.S.-led coalition in 2019—is presently seeing a resurgence in the wake of geopolitical events like the fall of the Assad regime.[7]

ISIS has continued to operate as a decentralized organization, which translates into a financial model that leans heavily into local revenue generation by affiliates. While ISIS Core[8] still has access to some cash reserves, estimates note this has dwindled to $10 million as of late 2024, down from $500 million at the height of the ISIS caliphate, necessitating more diverse sources of revenue.[9] Aside from cash reserves, ISIS branches exploit regional instability, local conflicts, and areas with weak governance to raise funds in their respective localities.[10] These revenue sources

5 With respect to information collected from pending cases, the charges contained in an indictment are merely allegations. A defendant is presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law.

6 The review period is January 1, 2024, to December 31, 2025.

7 Reuters, "American and Syrian forces conduct airstrikes on ISIS weapons storage facilities, US military says," (Nov. 30, 2025), https://www.reuters.com/business/aerospace-defense/american-syrian-forces-conduct-airstrikes-isis-weapon-storage-facilities-us-2025-11-30/.

8 "ISIS Core" refers to ISIS's original domain and sphere of influence in Syria and Iraq.

9 "Fact Sheet on ISIS Financing," (Aug. 8, 2024), https://home.treasury.gov/system/files/136/Fact-Sheet-on-ISIS-Financing.pdf (Fact Sheet on ISIS Financing).

10 Fact Sheet on ISIS Financing.

include collecting fundraising disguised as *zakat* (Islamic almsgiving), spoils of war, extortion, kidnapping for ransom, and international donations. African branches of ISIS—which are some of ISIS' most profitable and most important—such as ISIS-Somalia, ISIS-DRC, and ISIS-West Africa, raise hundreds of thousands of dollars per month through extortion schemes.[11] The Al-Siddiq Office, which oversees ISIS-K, and the Al-Karrar Office, which oversees ISIS-Somalia, continue to play important roles as regional hubs for funneling money to and from affiliates. Some reports have indicated that ISIS-K in particular has been increasingly reliant on international donations over other methods of fundraising.[12] Online fundraising efforts, both in fiat and digital assets, have continued to be heavily employed by ISIS.

ISIS continues to heavily utilize informal traditional methods of moving funds outside the regulated economy, such as cash and money transmitters. Notably, the ISIS branch in West Africa engages with the regulated financial sector by using bank accounts to transfer money.[13] Türkiye also continues to serve as an important intermediary transit point for fund transfers associated with the group. However, in 2024 and 2025, ISIS expanded its use of digital assets, including more organizational transfers and donations from international supporters.[14] ISIS has also used digital assets to fund external operations, such as the 2024 Crocus Hall attack in Moscow; reportedly ISIS-K transferred at least $2,000 in digital assets to the Crocus Hall attackers.[15] ISIS also continues to solicit digital asset donations online through Voice of Khorasan magazine, and has reportedly raised tens of thousands of dollars from international donors. In January 2024, Treasury's Office of Foreign Assets Control (OFAC) sanctioned two Egypt-based ISIS cybersecurity experts in part for providing guidance to ISIS leadership on the use of digital assets.[16]

Consistent with the findings of the 2024 NTFRA, the financial nexus to the United States is still mainly individual supporters sending money abroad using digital assets, MSBs, or cash, or attempting to travel abroad to fight on behalf of the group. ISIS remains the FTO most frequently identified in TF activity within the United States.[17] In the past two years, U.S. individuals have also attempted to provide other forms of support, such as recruitment; information on bomb-making, hacking, computer expertise, and cybersecurity; creation of propaganda and false identity documents; guns; or other materials.[18] Some U.S. individuals have also been accused and convicted of more extensive fundraising on behalf of the group.[19] For individuals looking to travel to join ISIS, U.S. persons have generally used cash or made travel arrangements using a credit card.

- In 2025, two U.S. residents, Ahmed Mahad Mohamed and Abdi Yemeni Hussein, were sentenced for conspiring to travel to Egypt for the purpose of fighting for ISIS in the Sinai Peninsula.[20] Beginning in at least August 2018, Mohamed sought out other ISIS supporters online, stating that he wanted to travel to ISIS-controlled territory to become "the beheading guy" and martyr himself. Mohamed also stated that his only dream was to go to Syria, join ISIS, and "fight jihad," and he indicated that his friend, Hussein, also desired to travel to ISIS territory abroad. Mohamed and Hussein met in person in 2019 to discuss their plans. Mohamed reiterated that his goal was to fight for ISIS abroad. Hussein told Mohamed that they would either reach ISIS territory "or we go to jail," and suggested attacking the White House if they were prevented from traveling. By June 2019, the defendants began making travel arrangements to join ISIS. They both sold their cars and purchased plane tickets from Tucson to Cairo. On the morning of July 26, 2019, the defendants checked in for their flight at the Tucson International Airport, went

11 Id.
12 United Nations Monitoring Team Thirty-fifth Report, (Feb. 2025), p. 20.
13 Fact Sheet on ISIS Financing.
14 Id.
15 Id.
16 Department of Treasury, OFAC, "Treasury Designates ISIS Cyber Facilitators and Trainers," (Jan. 30, 2024), https://home.treasury.gov/news/press-releases/jy2056.
17 Based on a comprehensive review of court indictments, prosecutions, and convictions.
18 See, e.g., Department of Justice, "Former Refugee Pleads Guilty and Admits to Supporting ISIS," (Mar. 7, 2025), https://www.justice.gov/opa/pr/former-refugee-pleads-guilty-and-admits-supporting-isis.
19 See e.g., Department of Justice, "Two Defendants Convicted of Conspiring to Provide Material Support to ISIS," (Oct. 24, 2025), https://www.justice.gov/opa/pr/two-defendants-convicted-conspiring-provide-material-support-isis.
20 Department of Justice, Two Tucson Men Sentenced for Conspiring to Travel to the Middle East to Fight for ISIS," (Jan. 23, 2025), https://www.justice.gov/usao-az/pr/two-tucson-men-sentenced-conspiring-travel-middle-east-fight-isis.

through security screening, and walked to the departure gate. Mohamed was carrying approximately $10,000 that he and Hussein planned to use for travel expenses and to buy firearms. Once in Egypt, the defendants intended to smuggle themselves into the ISIS-controlled area of the Sinai Peninsula so they could work under the direction and control of ISIS. Before Mohamed and Hussein could board their flight, the FBI arrested them.

- In May 2025, a Virginia man was sentenced to 30 years in prison on charges relating to his efforts to provide material support to ISIS.[21] According to court records and evidence presented at trial, from at least October 2019 through October of 2022, Mohammed Azharuddin 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 digital assets and send it to Türkiye, where it was smuggled to ISIS members in Syria. His primary co-conspirator was an 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 over $185,000 in digital assets.

Al-Qa'ida (AQ)

While AQ central leadership has been weakened on an organizational level, the U.S. Department of Homeland Security (DHS) has assessed that AQ maintains its commitment to attacking the U.S. homeland.[22] Similar to ISIS, AQ has been galvanized by the Israel-Hamas conflict and has encouraged supporters to conduct attacks on their own against the United States.[23] Some of AQ's leaders still reside in Iran and much of AQ's power resides with affiliate groups. In particular, AQ affiliates in Africa are on the ascent, and have continued to operate nearly autonomously, conducting destabilizing activities throughout parts of Africa and playing key roles in fundraising for the organization at large.

Al-Shabaab, an affiliate of AQ in Somalia, has grown in size, influence, and capability over the years and has demonstrated continued intent to attack U.S. interests. In 2024, an individual was convicted for conspiring to commit a 9/11-style attack at the direction of al-Shabaab, demonstrating al-Shabaab's capability and intent to commit attacks against the U.S. homeland.[24] Additionally, in 2024 and 2025, the United Nations (UN) noted increasing levels of cooperation between al-Shabaab and Ansar Allah, another U.S. designated FTO in Yemen supported by Iran, commonly known as the Houthis. Other affiliates of AQ are deeply entrenched in regional conflicts in Africa and have focused their efforts more locally. These affiliates include Jama'at al-Islam wal-Muslimin (JNIM), which has waged a strong insurgency campaign throughout Mali and West Africa and has gained territorial control and increased operational capabilities.[25]

AQ affiliates continue most historical methods of revenue generation, often exploiting vulnerable natural resources and financial opportunities that are available to them where they operate. These methods include extortion or taxation; and exploiting resources such as illicit timber logging, charcoal smuggling, and precious metals and stones, among others. This is particularly the case in countries where the government is unable to effectively exert control over large amounts of territory.

While AQ affiliates have varying degrees of sophistication in raising and moving funds, al-Shabaab is by far the most financially successful AQ affiliate, generating over $100 million per year through extortion of citizens, businesses, and individual contributions from affiliated businesspeople in Somalia. Some of these funds are redistributed to

21 Department of Justice, "Man Sentenced to Over 30 Years in Prison for Crypto-Terror Financing Scheme," (May 8, 2025), https://www.justice.gov/opa/pr/man-sentenced-over-30-years-prison-crypto-terror-financing-scheme.

22 Department of Homeland Security, Homeland Threat Assessment, Homeland Threat Assessment 2025, p. 4 (Oct. 2, 2024), https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.

23 Id.

24 Department of Justice, "Cholo Abdi Abdullah Convicted for Conspiring to Commit 9/11-Style Attack at the Direction of Al Shabaab," (Nov. 4, 2024), https://www.justice.gov/archives/opa/pr/cholo-abdi-abdullah-convicted-conspiring-commit-911-style-attack-direction-al-shabaab.

25 United Nations Monitoring Team Thirty-sixth Report, (Jul. 2025), p. 6.

other AQ-affiliated groups around the world.[26] In 2024, Treasury imposed sanctions on 16 entities and individuals who comprise an expansive business network spanning the Horn of Africa, the United Arab Emirates (UAE), and Cyprus that raises and launders funds for al-Shabaab.[27] Individuals within this network include influential businesspeople in the region who lend financial backing to al-Shabaab, and have been involved with raising and laundering millions of dollars for the benefit of al-Shabaab. These businesspeople span Africa and the Middle East, including connections in UAE, Uganda, Kenya, Cyprus, and Somalia.

AQ and its affiliates' TF connections within the U.S. have been limited in recent years. Historically, U.S.-based supporters have most often been observed sending funds to AQ affiliates, such as al-Shabaab, using registered MSBs or cash.

- In April 2024, a woman was sentenced to 18 years in prison for using digital assets to provide financial support to terrorist groups operating in Syria.[28] As proven at trial, from September 2018 through June 2019, Victoria Jacobs provided material support to a formerly designated AQ affiliate group[29] while living in New York City. Jacobs provided more than $6,000 to the terrorist training group "Malhama Tactical," which fought with and provided special tactical and military training for the group. Jacobs also laundered $12,000 on behalf of Malhama Tactical by receiving digital assets and wires from supporters around the globe and sending the funds to Bitcoin wallets controlled by Malhama Tactical. In addition to sending digital assets, she also purchased gift cards for the organization.
- In January 2024, an individual pleaded guilty to attempting to provide material support to a formerly designated AQ affiliate group. Between July 2020 and February 2021, he used money transfer services to send approximately $13,000 to two known couriers connected to the group. Records obtained from the money transfer services documented multiple transactions to the couriers in Türkiye, usually in increments of $1,000.[30]
- In January 2025, a U.S. citizen pleaded guilty to attempting to provide material support to al-Shabaab.[31] Starting at least in or about November 2023, he repeatedly expressed his desire and plans to join al-Shabaab, a designated FTO that has attacked Americans and American allies around the world, and wage jihad, including in communications with an FBI confidential source, who was posing as a facilitator for terrorist organizations. In communications with the CS, the individual expressed his intent to join al-Shabaab to receive military training and engage in jihad, that he was prepared to kill and be killed, and that he specifically aspired to be a martyr for the jihadist cause. He made social media posts warning that jihad would come to the United States, posting airplane, bomb, and emojis. The individual prepared to travel to Somalia by traveling first to Kenya, from which he booked a roundtrip flight and made hotel reservations in order to create the appearance he was traveling to Kenya as a tourist.

Hizballah

Hizballah has historically had one of the most extensive global operations and financial infrastructures of any terrorist group. However, in contrast to prior years, Hizballah has been degraded over the course of the Israel-Hamas war. In late 2024, Hizballah's longtime leader Hasan Nasrallah was killed in an Israeli bombing in Lebanon, marking a turning point for the group. Despite this significant setback, Hizballah still remains a potent military and political force in the region with the capability and intent to attack U.S. interests and personnel.

26 Id. p. 15.

27 Department of Treasury, OFAC, "Treasury Designates Transnational al-Shabaab Money Laundering Network," (Mar. 11, 2024), https://home.treasury.gov/news/press-releases/jy2168.

28 Manhattan District Attorney's Office, "D.A. Bragg: Victoria Jacobs Sentenced To 18 Years In Prison For Using Cryptocurrency To Fund Syrian-Based Terrorist Groups; Launder Supporters' Contributions," (Apr. 30, 2024), https://manhattanda.org/d-a-bragg-victoria-jacobs-sentenced-to-18-years-in-prison-for-using-cryptocurrency-to-fund-syrian-based-terrorist-groups-launder-supporters-contributions/.

29 A delisting does not retroactively negate any convictions for material support to prior to that date, and these cases remain important indicators of terrorist financing typologies in the United States.

30 Department of Justice, "Russian National Pleads Guilty to Attempting to Provide Material Support to a Foreign Terrorist Organization," (Jan. 8, 2024), https://www.justice.gov/archives/opa/pr/russian-national-pleads-guilty-attempting-provide-material-support-foreign-terrorist.

31 Department of Justice, "New Jersey Man Pleads Guilty To Attempting To Provide Material Support To Al Shabaab," (Jan. 27, 2025), https://www.justice.gov/usao-sdny/pr/new-jersey-man-pleads-guilty-attempting-provide-material-support-al-shabaab.

Hizballah continues to maintain a range of different sources of revenue that span the globe. Predominantly, Hizballah receives hundreds of millions of dollars—with historical estimates numbering $700 million—in direct state sponsorship from Iran, and it supplements this through illicit activities involving smuggling and trafficking, individual donations from sympathetic diaspora around the world, and commercial and semi-legitimate business enterprises. This diversity of revenue allows Hizballah to be resilient to contractions in financing from Iran during periods of financial difficulty for the Iranian regime. Hizballah relies on key financial facilitators throughout the world who may use their legitimate businesses to raise or launder funds for the group. Key jurisdictions, such as West Africa and Latin America, have also been important nodes in Hizballah's illicit financial networks. Hizballah maintains robust networks of sympathizers and financiers in these regions that serve as sources of funding.

Hizballah's finance team manages a variety of lucrative commercial projects and oil smuggling networks to generate and transfer revenue for Hizballah, often in conjunction with Iran's Islamic Revolutionary Guard Corps – Qods Force (IRGC-QF). The Hizballah finance team uses front companies to generate millions of dollars in revenue for Hizballah and support the group's terrorist activities while also allowing key associates and family members to enrich themselves through these commercial enterprises.[32] Hizballah also maintains control, either directly or indirectly, over complicit financial institutions and licensed and unlicensed money exchange houses in key jurisdictions, such as Lebanon, that it uses as conduits to move millions of dollars. Unlicensed money exchanges and exchange companies that fail to conduct adequate screening on their customers allow Hizballah to take advantage of Lebanon's largely cash-based economy to launder illicit money.[33] Hizballah also relies on bulk cash smuggling to move funds from Iran into Lebanon.[34]

Hizballah's financial footprint in the United States often relies on sanctions evasion or money laundering using the U.S. financial system. As illustrated by the case study below, a key typology that Hizballah uses to evade sanctions and access the U.S. financial system is formation of foreign-based front companies that are often owned by sympathizers or family members of Hizballah associates and members. Consistent with Treasury's analysis in past years, the complexity and global nature of Hizballah's financial schemes mean that it is more likely than other FTOs to intersect with the U.S. financial system and may be more likely to send funds into the United States.

- In 2025, an indictment was returned charging a dual U.S.-Lebanese citizen with conspiracy to provide material support to a designated FTO and conspiracy to launder money.[35] According to the indictment, the individual owned and operated a Lebanese company, identified in court records as Company 1, that acquired electronics equipment in the United States and resold it to other entities located primarily in the Middle East and Africa. As alleged in the indictment, one of his customers was Al Manar TV, a television station based in Lebanon that is owned and operated by Hizballah. The individual and Company 1 allegedly used a relative and others based in the United States as co-conspirators to purchase audio, video, and other equipment. The merchandise was then consolidated and shipped overseas, at which point some of it was sold to Al Manar TV or to front companies affiliated with Al Manar TV. The individual allegedly arranged for the purchase of these items in a convoluted manner designed to obscure the source of the funds and the intended destination of the items. The defendant allegedly made a payment in Lebanon that triggered a Florida-based co-conspirator to send structured money orders to U.S.-based co-conspirators. The money orders were purchased in amounts that evaded anti-money laundering (AML) regulations. In total, the defendant allegedly caused approximately $396,160 in structured money orders to be paid to U.S.-based co-conspirators.

32 Department of Treasury, "Treasury Targets Hizballah Finance Team Sanctions Evasion Network," (Mar. 28, 2025), https://home.treasury.gov/news/press-releases/sb0063.

33 Department of Treasury, "Treasury Sanctions Hizballah Operatives Exploiting Lebanon's Cash Economy," (Nov. 6, 2025), https://home.treasury.gov/news/press-releases/sb0308.

34 Department of Treasury, "Treasury Disrupts Financial Facilitation Network Supporting Hizballah Terrorists," (May 15, 2025), https://home.treasury.gov/news/press-releases/sb0143.

35 Department of Justice, "Dual citizen indicted for using Lebanese business to support Hizballah," (Jun. 5, 2025), https://www.justice.gov/usao-edva/pr/dual-citizen-indicted-using-lebanese-business-support-hizballah.

- In September 2024, Mohammad Bazzi pleaded guilty to conspiracy to conduct and to cause U.S. persons to conduct unlawful transactions with a Specially Designated Global Terrorist. Following Bazzi's OFAC designation in 2018, Bazzi and his co-defendant, Talal Chanine, who remains at large in Lebanon, conspired to force or induce an individual located in the United States to liquidate their interests in certain real estate assets located in Michigan and covertly transfer hundreds of thousands of dollars in proceeds of the liquidation out of the United States to Bazzi and Chahine in Lebanon without the required OFAC licenses, in violation of the International Emergency Economic Powers Act. During recorded communications, Bazzi and Chahine proposed numerous methods to conceal from OFAC and law enforcement officials that Bazzi was both the source and destination of the proceeds of the sale and to create the false appearance that the U.S. Person was conducting legitimate arms-length transactions unrelated to Bazzi and Chahine.[36]

Hamas

Hamas continues to pose a global threat but has been severely diminished, both financially and militarily, over the past two years due to the conflict with Israel and sustained international CT pressure in the wake of the October 7, 2023 attacks. Hamas has sought to fundraise from a wide range of global sources, including from donors in the United States. Disruption of recent plots in Europe illustrate the extent of the group's global facilitation networks, as well as its intent to plan external operations.[37] Despite financial hardships, key elements of its financial infrastructure remain intact, and the overall TF threat from Hamas remains high as the group will likely seek to shore up financial resources to reconstitute.

While Hamas has managed to retain some of its diverse sources of revenue since its October 7 terrorist attacks on Israel, some funding streams have been severely disrupted, resulting in financial hardships for the group. Hamas continues to rely on global fundraising efforts, donations, hundreds of millions of dollars in state sponsorship from Iran, and abuse of sham charitable entities for revenue. Prior to October 7, Hamas' secret international investment portfolio had been identified as an important element for Hamas to generate and store funds. This revenue stream has been impeded following U.S. sanctions and likely no longer represents the financial asset that it once did.

The fallout of the October 7 attacks exposed Hamas' global reliance on the abuse of sham charitable entities to raise funds.[38] Treasury has assessed that as of early 2024, Hamas may have received as much as $10 million a month through such donations.[39] In June 2025, a Treasury action exposed a number of sham charities operating throughout Türkiye, Algeria, the Netherlands, Italy, and the West Bank and Gaza.[40] Some of these entities were controlled outright by Hamas or those with ties to the group. While some of these entities clandestinely hid their support for Hamas and solicited donations under the guise of charitable work from unwitting donors, some explicitly called for donations for Hamas. Hamas also solicits funds online in other ways, including using social media and often encourages donations of digital assets. Hamas' use of digital assets for fundraising is demonstrated by two major seizures in 2025, discussed in more detail below.

Hamas continues to rely on networks of financial facilitators, cash couriers, and complicit financial institutions to move money around the region. Money exchangers play a key role in Hamas' financing infrastructure, illustrated, in part, by the fact that Israel has conducted military operations and airstrikes against Gaza-based money exchangers. The group also relies on bulk cash smuggling and the informal economy to move funds. Crucially, Hamas has also exploited complicit digital asset service providers in foreign jurisdictions to move funds.

36 Department of Justice, "Specially Designated Global Terrorist Mohammad Bazzi Pleads Guilty to Sanctions Evasion," (Sep. 20, 2024), https://www.justice.gov/usao-edny/pr/specially-designated-global-terrorist-mohammad-bazzi-pleads-guilty-sanctions-evasion.

37 See BBC, "Germany arrests suspected Hamas members over alleged attack plot," (Oct. 1, 2025), https://www.bbc.com/news/articles/cgknpzrkyvno.

38 Department of Treasury, "Treasury Disrupts Sham Overseas Charity Networks Funding Hamas and the PFLP," (Jun. 10, 2025), https://home.treasury.gov/news/press-releases/sb0162.

39 Department of Treasury, "Treasury Targets Significant International Hamas Fundraising Network," (Oct. 7, 2024), https://home.treasury.gov/news/press-releases/jy2632.

40 Department of Treasury, "Treasury Disrupts Sham Overseas Charity Networks Funding Hamas and the PFLP," (Jun. 10, 2025), https://home.treasury.gov/news/press-releases/sb0162.

Within the United States, financial connections to Hamas are limited, but the U.S. government continues to closely monitor any financial activity that may be linked to the group. Hamas has sought to raise funds from international donors through online international fundraising schemes and looks to raise funds from the widest array of sympathizers, including from those in the United States. Following Treasury's Financial Crimes Enforcement Network's (FinCEN) issuance of the Advisory on Hamas Financing[41] in 2023, 642 Suspicious Activity Reports (SARs) that include the key term specified in the Advisory have been filed by U.S. financial institutions, indicating that U.S. financial institutions observe continued potential connections to Hamas financing.[42]

- In March 2025, DOJ announced the disruption of an ongoing terrorist financing scheme through the seizure of approximately $201,400 in digital assets held in wallets and accounts intended to benefit Hamas.[43] As alleged in court documents, a group chat claiming association with Hamas on an encrypted communications platform provided Hamas supporters worldwide with a changing set of at least 17 digital asset addresses. Supporters were encouraged to donate money to those addresses. Those funds were sent into an operational wallet and laundered through a series of digital asset exchanges and transactions by leveraging suspected financiers and over-the-counter brokers. More than a million dollars was raised and laundered through this scheme using the laundering system and the related digital asset accounts described in the affidavit.
- In July 2025, DOJ and the U.S. Attorney's Office for the District of Columbia announced the unsealing of a civil forfeiture action against approximately $2 million dollars in digital currency connected with Buy Cash Money and Money Transfer Company (BuyCash), a Gaza-based money transfer business that was involved in financially supporting Hamas.[44] BuyCash, and one of its owners, Ahmed M. M. Alaqad, have been suspected of supporting various terrorist organizations including Hamas, ISIS, AQ affiliates, and others. After the October 7 attacks on Israel, BuyCash and Alaqad were designated as having materially supported Hamas under Executive Order (E.O.) 13224 by OFAC. Since 2017, BuyCash and Alaqad have supported several FTOs. In 2017, BuyCash was used for the procurement of large quantities of online infrastructure on behalf of ISIS. In September 2019, BuyCash was used to receive funds from a known AQ affiliate. In 2019, law enforcement identified various instances where BuyCash, with the direct support of Alaqad, directly aided in the transfer of fiat currency to known individuals and entities in support of Hamas. In June 2021, Israel's National Bureau for Counter Terrorist Financing seized various digital currency accounts connected to Hamas and the Izz-al-Din Qassam Brigades, including one involving BuyCash. The complaint describes a detailed scheme whereby users utilized BuyCash to fund digital asset exchange accounts and unhosted wallets to obfuscate their financial support of international terrorist organizations, including Hamas. Before and after the October 7 attacks, one account was reported to have received at least $4 million to support Hamas.

Homegrown Violent Extremists (HVEs)

Individuals in the United States who are inspired by an FTO and radicalized online to conduct domestic attacks, (sometimes referred to as HVEs) are one of the primary terrorism threats to the United States.[45] Various FTOs, including ISIS, have increasingly praised and publicly advocated for these types of lone offender attacks in their propaganda material.[46] These attacks remain incredibly challenging to proactively detect, as there is generally no outside financing involved and individuals typically use easy to acquire weapons, such as edged weapons

41 Department of Treasury, "FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities," (Oct. 20, 2023), https://www.fincen.gov/system/files/2023-10/FinCEN_Alert_Terrorist_Financing_FINAL508.pdf.

42 Current as of January 28, 2026.

43 Department of Justice, "Justice Department Disrupts Hamas Terrorist Financing Scheme Through Seizure of Cryptocurrency," (Mar. 27, 2025), https://www.justice.gov/opa/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure-cryptocurrency.

44 Department of Justice, "United States Unseals Civil Action Filed Against Approximately $2M in Digital Currency Involved in Hamas Fundraising," (Jul. 22, 2025), https://www.justice.gov/opa/pr/united-states-unseals-civil-action-filed-against-approximately-2m-digital-currency-involved.

45 "Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, Before the Committee on the Judiciary, United States Senate,"(Dec. 5, 2023), https://www.judiciary.senate.gov/imo/media/doc/2023-12-05_-_testimony_-_wray.pdf; Federal Bureau of Investigation, "Investigative Updates on the New Orleans Bourbon Street Attack," (Jan. 5, 2025), https://www.fbi.gov/news/speeches-and-testimony/investigative-updates-on-the-new-orleans-bourbon-street-attack-010525.

46 Id.

and firearms, to conduct low-cost but deadly attacks against pedestrians, law enforcement, military members, or crowded public venues.[47] These attacks are generally self-funded through the perpetrator's own employment or personal savings. Recently, the 2025 New Years Day attack in New Orleans demonstrated the lethality and relative ease with which these attacks can be carried out. In this instance, the individual was radicalized online by ISIS propaganda to commit an attack. He traveled to New Orleans in a rental truck, obtained a short-term rental property, and placed improvised explosive devices (IEDs) at various locations near major thoroughfares in downtown New Orleans before using his rental truck as a weapon and driving into a crowd celebrating the New Year.

According to analysis of the Bank Secrecy Act (BSA) data relating to HVE activity by FinCEN, 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.[48] Other indicators may include sudden account closures and disbursements as well as the sudden urgent liquidation of valuable personal assets without apparent concern for financial gain.

For example, in June 2025, a native and citizen of Afghanistan pleaded guilty in federal court in Oklahoma City to two terrorism-related offenses: conspiring and attempting to provide material support and resources to ISIS and receiving, attempting to receive, and conspiring to receive firearms and ammunition in furtherance of a federal crime of terrorism. According to court documents, Nasir Ahmad Tawhedi admitted that between June 2024 and October 2024, he conspired with at least one other individual to purchase two AK-47 rifles, 500 rounds of ammunition, and 10 magazines, with the intent to carry out a mass-casualty attack on or around Election Day, November 5, 2024, on behalf of ISIS. Tawhedi also allegedly accessed, viewed, and saved ISIS propaganda on his iCloud and Google account, participated in pro-ISIS Telegram groups, and contributed to a charity which fronts for and funnels money to ISIS. Tawhedi took steps to liquidate his family's assets prior to the attack, and his co-conspirator advertised the sale of the family's personal property on Facebook.[49] Tawhedi sold his family's house for approximately $185,000, as well as their two vehicles, furniture, electronics, and other personal property and intended to use the money to acquire assault rifles, magazines, and ammunition and to resettle and repatriate his family to Afghanistan.[50]

Domestic Violent Extremists (DVEs)

Consistent with the 2024 NTFRA's findings, violence and terrorist acts by Domestic Violent Extremists (DVEs) have remained a threat to the U.S. homeland. To combat DVE threats, on September 25, 2025, President Trump issued the National Security Presidential Memorandum (NSPM)-7, which creates a "new national strategy to investigate and disrupt networks, entities, and organizations that foment political violence so that law enforcement can intervene in criminal conspiracies before they result in violent political acts."[51]

A DVE is an individual based and operating primarily in the United States, without direction from an FTO or other foreign power, who seeks to further political or social goals wholly or in part through unlawful acts of force or violence. DVE activity is driven by a wide range of ideological, personal, and sociopolitical grievances, and DVE actors are often inconsistent in their beliefs.

47 IC3, "PSA: Threat of Copycat Attacks after ISIS-Inspired Vehicle Attack in New Orleans," (Jan. 13, 2025), https://www.ic3.gov/PSA/2025/PSA250113.

48 FinCEN, "FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates," (Apr. 1, 2025), https://www.fincen.gov/system/files/advisory/2025-04-01/FinCEN-Advisory-ISIS-508C.pdf.

49 Department of Justice, "Afghan National Pleads Guilty to Plotting Election Day Terror Attack in the United States," (Jun. 13, 2025), https://www.justice.gov/opa/pr/afghan-national-pleads-guilty-plotting-election-day-terror-attack-united-states.

50 Criminal Complaint, USA v. Tawhedi, Case No. 5:24-mj-00760, W.D.Ok, (Oct. 8, 2024), available at https://www.justice.gov/archives/opa/media/1373021/dl.

51 The White House, "Countering Domestic Terrorism and Organized Political Violence," (Sep. 25, 2025), https://www.whitehouse.gov/%20presidential-actions/2025/09/countering-domestic-terrorism-and-organized-political-violence/.

Historically, DVEs motivated by exclusionary, or absolutist belief systems – including those rooted in racial or ethnic beliefs, religious extremism, anti-government ideologies, and identity-based movements – have posed a recurring threat of both lethal and non-lethal violence against religious, cultural, commercial, and government targets. In recent years, however, the domestic threat landscape has continued to diversify. This includes an increase in violent activity by individuals who lack a coherent or traditional ideological framework and instead espouse beliefs centered on nihilism, societal collapse, or the rejection of established social order, commonly referred to as "nihilistic" violent extremists. DVEs promoting accelerationist ideology—an ideology that seeks to destabilize society and trigger societal collapse—have continued to focus physical attacks on infrastructure and other critical functions, including attacks against the energy, communications, and public health sectors.

The United States also remains concerned about the influence that transnational terrorist groups have on DVE actors. For example, on November 13, 2025, the U.S. Department of State designated four violent "Antifa" groups—Antifa Ost, Informal Anarchist Federation/International Revolutionary Front (FAI/FRI), Armed Proletarian Justice, and Revolutionary Class Self-Defense— as SGDTs and subsequently designated all four as FTOs, effective November 20, 2025.[52] These groups operate as transnational networks that promote and carry out violent attacks against perceived political adversaries and government-related targets, including assaults, arson, and the use of improvised explosive devices.[53]

In January 2025, the U.S. Department of State designated the Terrorgram Collective as a Specially Designated Global Terrorist (SDGT). The Terrorgram Collective is a transnational terrorist network that primarily operates through online platforms, including the social media and digital messaging application Telegram. The group promotes violent, exclusionary, and identity-based extremist ideologies; actively solicits attacks against perceived adversaries; and disseminates guidance and instructional materials related to tactics, methods, and target selection, including against critical infrastructure and government officials. The group also glorifies individuals who have carried out acts of violence consistent with its messaging. Attacks or attempted attacks motivated or facilitated by Terrorgram Collective adherents include an October 2022 shooting outside an LGBT bar in Slovakia; a July 2024 disrupted plot targeting energy facilities in New Jersey; and an August 2024 knife attack at a mosque in Türkiye.

Although primarily based overseas, these groups rely heavily on online platforms to disseminate propaganda, share operational guidance, glorify prior acts of violence, and encourage follow-on attacks, increasing the risk that their tactics, messaging, or facilitation efforts may influence or inspire violent activity connected to the United States. The designations reflect the U.S. government's assessment that these groups engage in terrorist activity and pose a continuing threat to international security, while also underscoring broader concerns about the convergence between transnational extremist networks and domestic violent extremist actors.[54] The United States continues to monitor potential financial, logistical, and ideological linkages between these designated groups and individuals or supporters operating domestically, particularly where online engagement, self-financing, or small-dollar transactions could be used to support or encourage acts of violence.

DVEs in the United States continue to operate primarily as lone-wolves or in small groups, using self-financing methods to conduct attacks. Distinct from the large, organized terrorist groups, if DVEs raise funds, it is generally done through licit activity. These funds may later be surreptitiously used to support violent extremist activities rather than for the purported fundraising cause. However, most often, those seeking to commit attacks are acting by themselves and utilize their own personal income or savings.

Given this fact pattern, it is extremely difficult for law enforcement and financial institutions to identify suspicious activity ahead of an attack. DVEs also often operate in relatively small dollar amounts, making suspicious activity even more difficult to detect. Given these challenges for law enforcement and financial institutions, the risk posed by DVEs continues to be significant.

52 Department of State, "Designations of Antifa Ost and Three Other Violent Antifa Groups," (Nov. 13, 2025), https://www.state.gov/releases/office-of-the-spokesperson/2025/11/designations-of-antifa-ost-and-three-other-violent-antifa-groups.

53 Id.

54 Id.

- In January 2025, Casey Robert Goonan pleaded guilty to one count of maliciously damaging or destroying property used in or affecting interstate commerce by means of fire or an explosive. According to the plea agreement, on June 1, 2024, Goonan placed a bag containing six explosive devices underneath the fuel tank of a marked University of California Police Department patrol car parked near the University of California (UC) Berkeley campus and lit the bag on fire, causing the patrol car to catch on fire. Goonan also attempted to firebomb the Ronald V. Dellums Federal Building and a U.S. Courthouse in Oakland, California, although this attempt was disrupted by protective services officers, and lit several other fires around the UC Berkeley campus. Goonan acknowledged that these attacks were inspired by Hamas's October 7 attacks on Israel, and that he called on others to attack property on Bay Area college campuses in support of Palestine. He further admitted that his conduct was designed to influence and affect the conduct of governments by intimidation and coercion and to retaliate against the governments of the United States and the State of California for their conduct. In September 2025, Goonan was sentenced to serve 235 months in federal prison, followed by 15 years of supervised release and was ordered to pay restitution of approximately $94,000.[55]
- In August 2025, the Department of Justice announced that Dallas Humber, a senior leader of the Terrorgram Collective, pleaded guilty to all charges against her.[56] In connection with her guilty plea, Humber admitted that from July 2022 until her arrest in September 2024, she served in a leadership role within the Terrorgram Collective, a transnational terrorist network that promotes and facilitates acts of violence. Humber and other members of the Terrorgram Collective solicited individuals to commit violent crimes, including attacks against critical infrastructure and targeted assassinations, and provided technical, inspirational, and operational guidance intended to enable those individuals to plan, prepare for, and carry out such attacks. Individuals motivated or facilitated by Humber and the Terrorgram Collective committed, attempted, or plotted attacks in the United States and abroad, including plots targeting energy facilities in New Jersey and Tennessee; the murder of two individuals in Wisconsin in furtherance of plans to assassinate a federal official; and an attempted assassination of an Australian official. On December 17, 2025, Humber was sentenced to 360 months' imprisonment.[57]

Special Focus: Cartels

Transnational drug cartels have continued to wage brutal campaigns of violence and intimidation in the United States. These cartels, responsible for trafficking massive amounts of fentanyl, cocaine, methamphetamine, and other drugs into the United States through the southern border, maintain organized militaristic groups to fight each other for control of drug trafficking territory and to silence those who oppose their illicit activities. In addition to drug trafficking, cartels are also routinely involved in human trafficking and smuggling; arms trafficking, robbery, timeshare fraud, oil and fuel smuggling, kidnapping, extortion, bribery, targeted killings, and other alternative

55 Department of Justice, "Domestic Terrorist Sentenced to More Than 19 Years in Prison for Firebombing University Police Car and Attempting to Firebomb Oakland Federal Building," (Sep. 24, 2025), https://www.justice.gov/opa/pr/domestic-terrorist-sentenced-more-19-years-prison-firebombing-university-police-car-and.

56 Department of Justice, "Leader of Transnational Terrorist Group Pleads Guilty to Soliciting Hate Crimes, Soliciting the Murder of Federal Officials, and Conspiring to Provide Material Support to Terrorists," (Aug. 8, 2025), https://www.justice.gov/opa/pr/leader-transnational-terrorist-group-pleads-guilty-soliciting-hate-crimes-soliciting-murder.

57 Department of Justice, "Leader of Transnational Terrorist Group Sentenced to 30 Years in Prison for Soliciting Hate Crimes and Murder, and Conspiring to Provide Material Support to Terrorists," (Dec. 17, 2025), https://www.justice.gov/opa/pr/leader-transnational-terrorist-group-sentenced-30-years-prison-soliciting-hate-crimes-and.

revenue sources and acts of violence to further their operations.[58] Since January 2025, it has been the explicit policy of the United States to pursue the total elimination of these organizations and their ability to threaten the territory, safety, and security of the United States through their extraterritorial command-and-control structures.[59]

Since February 2025, State has designated 15 international cartels and other organizations—Cártel del Noreste (CDN), Tren de Aragua (TdA), Mara Salvatrucha (MS-13), Cartel de Sinaloa, Cartel de Jalisco Nueva Generación (CJNG), La Nueva Familia Michoacana (LNFM), Cartel del Golfo (CDG), Clan del Golfo, Carteles Unidos (CU), Gran Grif, Viv Ansanm, Los Lobos, Los Choneros, Barrio 18, and Cartel de los Soles—as FTOs and/or SDGTs.[60] Subsequently, OFAC designated various leaders of these cartels as SDNs pursuant to E.O. 14059, which targets the proliferation of illicit drugs and their means of production, and pursuant to E.O. 13224, as amended, which targets terrorists and their supporters. These designations have included, among others, two leaders of Los Chapitos, a faction of Cartel de Sinaloa (Sinaloa Cartel),[61] five leaders of CJNG,[62] two leaders of CDN,[63] four leaders of LNFM,[64] and 13 individuals and organizations that launder money for Sinaloa.[65] In addition, State, through its Narcotics Rewards Program and Transnational Organized Crime Rewards Program, has offered multi-million-dollar rewards for members of 11 of the 15 FTO-designated cartels/TCOs named since February.[66] Leaders of these cartels and TCOs have also been criminally charged in the United States, with three leaders of the Sinaloa Cartel, Ismael Zambada Garcia, Ovidio

58 FinCEN, "Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids," (Jun. 20, 2024), https://www.fincen.gov/sites/default/files/advisory/2024-06-20/FinCEN-Supplemental-Advisory-on-Fentanyl-508C.pdf; FinCEN, "Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids," (Aug. 21, 2019), https://www.fincen.gov/system/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf; FinCEN, "Financial Trend Analysis on Fentanyl-Related Illicit Finance: 2024 Threat Pattern & Trend Information," (Apr. 2025) https://www.fincen.gov/sites/default/files/shared/FinCEN-FTA-Fentanyl.pdf; FinCEN, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (Oct. 15, 2020) https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory Human Trafficking 508 FINAL_0.pdf; FinCEN, "Alert on Human Smuggling along the Southwest Border of the United States," (Jan. 13, 2023), https://www.fincen.gov/system/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf; FinCEN, "FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations," (July 16, 2024) https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf; FinCEN, "Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels," (May 1, 2025), https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Oil-Smuggling-FINAL-508C.pdf.

59 The White House, "Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists," (Jan. 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/designating-cartels-and-other-organizations-as-foreign-terrorist-organizations-and-specially-designated-global-terrorists.

60 Department of State, "Designation of International Cartels," (Feb. 20, 2025) https://www.state.gov/designation-of-international-cartels; Department of State, "Terrorist Designations of Viv Ansanm and Gran Grif," (May 2, 2025), https://www.state.gov/releases/office-of-the-spokesperson/2025/05/terrorist-designations-of-viv-ansanm-and-gran-grif; Department of State, "Terrorist Designations of Los Choneros and Los Lobos," (Sep. 4, 2025), https://www.state.gov/releases/2025/09/terrorist-designations-of-los-choneros-and-los-lobos; Department of State, "Terrorist Designation of Barrio 18," (Sep. 23, 2025), https://www.state.gov/releases/office-of-the-spokesperson/2025/09/terrorist-designation-of-barrio-18/; Department of State, "Terrorist Designations of Cartel de los Soles," (Nov. 16, 2025), https://www.state.gov/releases/office-of-the-spokesperson/2025/11/terrorist-designations-of-cartel-de-los-soles/; Department of State, "Terrorist Designations of Clan del Golfo," (Dec. 16, 2025), https://www.state.gov/releases/office-of-the-spokesperson/2025/12/terrorist-designations-of-clan-del-golfo.

61 Department of Treasury, "Treasury Sanctions 'El Chapo's' Children and Los Chapitos, a Fentanyl-Trafficking Faction of the Sinaloa Cartel," (Jun. 9, 2025), https://home.treasury.gov/news/press-releases/sb0161.

62 Department of Treasury, "Treasury Sanctions Cartel de Jalisco Nueva Generacion Leaders Under Counterterrorism Authorities," (Jun. 18, 2025), https://home.treasury.gov/news/press-releases/sb0169.

63 Department of Treasury, "Treasury Sanctions High-Ranking Members of Foreign Terrorist Organization Cartel del Noreste," (May 21, 2025), https://home.treasury.gov/news/press-releases/sb0146.

64 Department of Treasury, "Treasury Sanctions Leaders of La Nueva Familia Michoacana Drug Cartel," (Apr. 15, 2025), https://home.treasury.gov/news/press-releases/sb0087.

65 Department of Treasury, "Treasury Sanctions Criminal Operators and Money Launderers for the Notorious Sinaloa Cartel," (Mar. 31, 2024), https://home.treasury.gov/news/press-releases/sb0064.

66 Id.

Guzman Lopez, and Joaquin Guzman Lopez;[67] and two leaders of Cartel de Los Soles, Hugo Carvajal Barrios and Clíver Alcalá Cordones,[68] pleading guilty to federal drug charges.

While these cartels have waged campaigns of fear and committed terrorist acts aimed at civilians and government officials from a financial perspective, their operations are distinctly different from other terrorist organizations. These groups are highly sophisticated organizations, raise massive amounts of funds through narcotics sales and other illicit activity to fund their global operations, and employ numerous typologies to launder the illicit proceeds through the U.S. financial system, including bulk cash smuggling, structured cash deposits into bank accounts; money transfers through P2P payment services and MSBs, trade-based money laundering, digital assets, and increasing use of professional money laundering networks such as Chinese money laundering networks.[69] This is in contrast to traditional forms of terrorist financing, where networks are highly insular, money laundering is generally done in-house, volumes of money are much lower, and funds intersecting with the U.S. financial system are usually low dollar amounts.

Treasury has long monitored the cartels' financing activities in the National Money Laundering Risk Assessments. Please see the 2026 National Money Laundering Risk Assessment for the most recent assessment of their money laundering practices.

- On March 11, 2025, FinCEN issued a Geographic Targeting Order to further combat the illicit activities and money laundering of Mexico-based cartels and other criminal actors along the southwest border of the United States.[70] The Order requires certain MSBs located in specific ZIP codes across Arizona, California, and Texas near the southwest border to file Currency Transaction Reports with FinCEN at a $1,000 threshold, in connection with cash transactions.[71]
- On October 6, 2025, OFAC sanctioned eight Mexican individuals and 12 Mexico-based companies affiliated with the Sinaloa Cartel's Los Chapitos faction. OFAC identified that this network supplies illicit fentanyl precursor chemicals to the Sinaloa Cartel, a terrorist organization responsible for a significant portion of the deadly drugs trafficked into the United States.[72]

---

67 Department of Justice, "Co-Founder of the Sinaloa Cartel, Ismael 'El Mayo' Zambada Garcia, Pleads Guilty to Engaging in a Continuing Criminal Enterprise and Racketeering," (Aug. 25, 2025), https://www.justice.gov/opa/pr/co-founder-sinaloa-cartel-ismael-el-mayo-zambada-garcia-pleads-guilty-engaging-continuing; Department of Justice, "Ovidio Guzman Lopez—Son of "El Chapo" and a Head of Sinaloa Cartel—Pleads Guilty to Federal Drug Charges in Chicago," (Jul. 11, 2025), https://www.justice.gov/usao-ndil/pr/ovidio-guzman-lopez-son-el-chapo-and-head-sinaloa-cartel-pleads-guilty-federal-drug; Department of Justice, "Joaquin Guzman Lopez — Son of 'El Chapo' and a Leader of Sinaloa Cartel — Pleads Guilty to Federal Drug Charges in Chicago," (Dec. 2, 2025), https://www.justice.gov/opa/pr/joaquin-guzman-lopez-son-el-chapo-and-leader-sinaloa-cartel-pleads-guilty-federal-drug.

68 Department of Justice, "Former Venezuelan General Pleads Guilty To Narco-Terrorism, Weapons, And Drug Trafficking Charges," (Jun. 25, 2025), https://www.justice.gov/usao-sdny/pr/former-venezuelan-general-pleads-guilty-narco-terrorism-weapons-and-drug-trafficking; Department of Justice, "Former Venezuelan General Sentenced To 260 Months In Prison For Providing Material Support To The FARC," (Apr. 8, 2025), https://www.justice.gov/usao-sdny/pr/former-venezuelan-general-sentenced-260-months-prison-providing-material-support-farc.

69 Taken from 2024 NMLRA p 52. See also FinCEN, "FinCEN Advisory: Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids" (Aug. 21, 2019), https://www.fincen.gov/system/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf; FinCEN, "FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations" (Mar. 31, 2025), https://www.fincen.gov/system/files/shared/BCS-Alert-FINAL-508C.pdf; FinCEN, "Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds," (Aug. 28, 2025), https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf; FinCEN, Financial Trend Analysis, "Chinese Money Laundering Networks: 2020 – 2024 Threat Pattern & Trend Information" (Aug. 28, 2025), https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

70 FinCEN, "FinCEN Issues Southwest Border Geographic Targeting Order," (Mar. 11, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-southwest-border-geographic-targeting-order.

71 FinCEN, "FinCEN Issues Modified Southwest Border Geographic Targeting Order," (Sep. 8, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-modified-southwest-border-geographic-targeting-order.

72 Department of Treasury, "Treasury Sanctions Illicit Fentanyl Supply Network Supporting the Sinaloa Cartel," (Oct. 6, 2025), https://home.treasury.gov/news/press-releases/sb0272.

VULNERABILITIES

Vulnerabilities can be exploited in the U.S. financial system to facilitate TF, both in the raising of funds for terrorist networks and attacks and the movement of funds to terrorists and terrorist organizations. As discussed below, MSBs, banks, online fundraising, P2P payment services, cash, digital assets, and misuse of the non-profit organizations (NPO) sector present vulnerabilities for TF.

Money Services Businesses (MSBs)

Registered MSBs play an integral role in the non-bank financial institution ecosystem. MSBs handle billions of dollars in legitimate transactions globally, providing financial services to unbanked and underbanked individuals who otherwise would not have access to the regulated financial sector. MSBs also allow for technological development and financial innovation, helping to drive new economic opportunities and provide greater financial services for large swaths of the public, including those already using the banking system. The use of MSBs for non-bank online payment services has grown and continues to grow rapidly in the United States.

Several factors make MSBs vulnerable to TF. As identified in past NTFRAs, by their nature, MSBs can move funds quickly and efficiently through the global financial system; may not require customers to open an account nor are they always required to verify identification for certain transactions; and may have operations in areas near conflict zones that are not served by banks. MSBs in the United States may also be exposed to risk from foreign agents or MSBs with whom they partner to provide services abroad.

Commensurate with the use of MSBs for money transferring purposes across all populations, terrorist groups have similarly sought to use these businesses to move funds, making MSBs a continued vulnerability. The continued use of MSBs for possible TF is evidenced by the scope of TF-related SARs filed by MSBs. MSBs regularly file more than half of all TF SARs (i.e., SARs reported with the "Known or Suspected Terrorist/Terrorist Organization" and "Other Terrorist" activities identified). In 2024, MSBs filed 924 SARs related to terrorist financing, representing 50% of all TF SARs.[73]

MSBs remain attractive to terrorist actors because they allow rapid, efficient movement of funds to underbanked areas. Domestically, the prevalence of certain MSBs for use in person-to-person payments has resulted in supporters of terrorist groups relying on their services. This is most commonly observed with individuals sending funds to affiliates of AQ or ISIS.

Registered MSBs are subject to AML/CFT regulation, including ongoing supervisory oversight and disclosure requirements at both the federal and state levels. These disclosure requirements, combined with market entry requirements, ensure that Treasury and individual state regulators generally have a clear and transparent understanding of the operations, ownership, and control of any individual MSB.

In the United States, some businesses may choose to engage in money transmitting or other services that would qualify them as an MSB under federal law but fail to comply with registration and regulatory requirements. Unregistered MSBs therefore evade AML/CFT oversight and present a risk for illicit activity, including TF. Recently, this activity has included digital asset service providers that operate without registering as MSBs. However, the risk stemming from unregistered MSBs has been reduced over the years due to stringent enforcement actions and consistent prosecution of this activity.

Outside of the United States, MSBs also play an important role in the global financial ecosystem by allowing those in financially disconnected areas to move and send money. In other jurisdictions where unregistered MSBs are prevalent, this can present significant TF risk. These financial transfers may not intersect with the regulated banking system, particularly in more traditional forms of money transmission, such as hawala. Although these

73 See FinCEN SAR Stats, https://www.fincen.gov/reports/sar-stats.

transactions may originate and settle outside the United States, they can still pose a risk to the U.S. financial system if funds ultimately transit through U.S. correspondent accounts, involve U.S.-based intermediaries, or support terrorist activity with implications for U.S. interests. Hawala-style services, in particular, have been exploited by groups such as AQ, ISIS, Hamas, and Hizballah to facilitate cross-border fund movement while evading scrutiny by regulated financial institutions.

Banks

In the United States and globally, banks[74] continue to serve as the primary vectors of finance. As described in previous NTFRAs, U.S. banks facilitate the majority of transactions that are processed on a day-to-day basis throughout the global financial system. Given the role of banks, the sheer volume of daily transactions in the banking sector, and the risks associated with U.S. banks' roles in foreign correspondent banking, U.S. and global banks' exposure to illicit activity overall, including terrorist financing, results in high overall inherent risks.

Commensurate with this risk, U.S. banks are subject to strong regulation by the banking supervisors and are regularly examined for their compliance with AML/CFT regulatory requirements. Most U.S. banks continue to have reasonably designed AML/CFT programs in place that comply with the BSA and AML/CFT regulatory requirements. These banks maintain mature, sophisticated customer and transaction monitoring practices and conduct appropriate risk-based due diligence to mitigate TF risks. Given these measures, backed by strong supervision by the bank regulators in the United States, banks are not assessed to be major conduits of terrorist financing in the U.S.

Nonetheless, large terrorist organizations—such as Hamas and Hizballah—have sought to use the U.S. banking system to store or move funds, often circumventing customer monitoring through the use of third parties and foreign-based front companies.[75] Further, smaller groups and individual terrorists have used banking services, particularly when funds are generated through licit sources. Abroad, terrorist groups have also been able to use the banking sector, particularly in territories under control of the terrorist groups or in jurisdictions with weak AML/CFT regimes.

Complacency and lack of proper investment into the necessary controls to combat TF can increase the risks for institutions. This was demonstrated when, in October 2024, the DOJ,[76] FinCEN,[77] and the Office of the Comptroller of the Currency[78] brought related criminal and civil enforcement actions against Toronto Dominion Bank (TD Bank) for multiple violations of the Bank Secrecy Act (BSA). The enforcement actions identified a number of critical lapses in TD Bank's AML/CFT compliance program, which ultimately led to several failures in appropriate customer and transaction monitoring. Among the many AML/CFT failures identified in these enforcement actions, the settlements identified that TD Bank allowed accounts to be opened for a New York-based religious institution, despite its leader's ties to terrorist organizations and involvement as an unindicted co-conspirator in the 1993 World Trade Center bombings, failed to perform adequate due diligence at account opening, and failed to understand its customers' terrorism-related associations. TD Bank ultimately reported on the customer but acknowledged that the suspicious activity indicative of terrorist financing began four years prior, shortly after the customer was onboarded. By the time the Bank reported, it had processed over $3 million in suspicious transactions for this customer, including deposits from crowdfunding platforms, charitable institutions, donations from individuals and businesses, unknown remitters utilizing a West Africa-based MSB and bulk cash and check deposits totaling

74 Banks refers to commercial banks, private banks, savings banks, industrial banks, savings and loan associations, and credit unions organized under the law of any state or of the United States. See 31 C.F.R. 1010.100(d).

75 See FATF, "FATF Report: Comprehensive Update on Terrorist Financing Risks," https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf, at p.50, noting that this is "less common than cash reserves."

76 Department of Justice, "TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations in $1.8B Resolution," (Oct. 10, 2024), https://www.justice.gov/archives/opa/pr/td-bank-pleads-guilty-bank-secrecy-act-and-money-laundering-conspiracy-violations-18b.

77 FinCEN, "FinCEN Assesses Record $1.3 Billion Penalty against TD Bank" (Oct. 10, 2024), https://www.fincen.gov/news/news-releases/fincen-assesses-record-13-billion-penalty-against-td-bank.

78 OCC, "OCC Issues Cease and Desist Order, Assesses $450 Million Civil Money Penalty, and Imposes Growth Restriction Upon TD Bank, N.A. for BSA/AML Deficiencies," (Oct. 10, 2024), https://www.occ.treas.gov/news-issuances/news-releases/2024/nr-occ-2024-116.html.

approximately $1 million from possible shell companies. As a result of delays in identifying and reporting the customer's activities, the Bank failed to detect and report these indicators of terrorist financing sooner, depriving law enforcement of an opportunity to intervene earlier. Through these enforcement actions, TD Bank ultimately pleaded guilty to conspiring to (1) fail to maintain an adequate AML Program; (2) fail to file accurate Currency Transaction Reports, and (3) launder monetary instruments;[79] and was assessed a record $3 billion in penalties.

Online Fundraising

Online fundraising continues to be a source of revenue for many terrorist groups, in particular for Hamas and ISIS, who have both sought to take advantage of witting and unwitting donors around the world. These groups may solicit funds directly via social media, advertising virtual asset wallet addresses, or P2P payment links. Additionally, as social media and companies have integrated new methods of payment into their platforms, new opportunities have emerged for sending funds. Social media platforms have also played an increasing role in allowing terrorists to network with each other online. In practice, recent cases have demonstrated domestic supporters of FTOs using social media to find and communicate with like-minded supporters or fellow extremists and then moving communication to encrypted messaging applications to facilitate the actual fundraising. Once on a secure platform, they may establish channels or group chats with those like-minded supporters and then disseminate payment links.

In 2025, two defendants were convicted of extensive online fundraising on behalf of ISIS.[80] They used Bitcoin, P2P platforms, and online crowdfunding platforms to raise funds, and then sent them to a known ISIS facilitator using an MSB. In early April 2021, members of a group chat on an encrypted messaging application discussed posting links that purported to be raising funds for humanitarian causes, but from which the money would actually be diverted to help the "mujahideen," an Arabic term used by ISIS supporters to refer to ISIS fighters. The defendants disseminated links to fiat accounts and digital asset wallets that were associated with ISIS. They also took operational security measures, with the ISIS facilitator instructing one of the defendants to delete messages and change his IP address. This case illustrates how fundraising methods using both fiat and digital assets may be combined through layered typologies to create a complex and diversified money trail. The defendants transferred approximately $35,000 in total to the ISIS facilitator and his associates.

Peer-To-Peer (P2P) Payments

P2P payment platforms allow users to transfer funds through mobile or desktop applications using linked bank accounts, prepaid cards, debit cards, stored balances, and, in some cases, credit cards for a fee. These platforms typically operate at low or no cost and facilitate rapid transfers, characteristics that can be exploited to move small dollar amounts quickly between individuals. P2P services generally function as closed-loop environments, meaning funds can only be sent to other users on the same platform, which may limit transparency and complicate the detection of illicit fundraising or fund movement conducted through multiple accounts.

In the United States, P2P payments remain a popular choice for rapid, efficient payments between two parties. These payment channels and platforms play an important role in accessibility and financial inclusion for populations around the world, particularly for those in financially disconnected regions who may be unable to access traditional banks and banking services. In the United States, providers of P2P payment services are often regulated as MSBs.

As P2P payments have permeated the economy and become a popular choice in households across the United States, they have also become a method for domestic supporters to send funds to FTOs. In some cases where individuals seek to do more extensive fundraising, funds may be gathered from many sources and then sent abroad using P2P channels or platforms. In some cases, the supporter or sender of funds may take steps to prevent these

79 Plea Agreement, USA v. TD Bank, N.A., Case No. 2:24-cr-00667, D.NJ (Oct. 10, 2024), available at https://www.justice.gov/archives/opa/media/1373336/dl.

80 Department of Justice, "Two Defendants Convicted of Conspiring to Provide Material Support to ISIS," (Oct. 24, 2025), https://www.justice.gov/opa/pr/two-defendants-convicted-conspiring-provide-material-support-isis.

payments from looking suspicious, for example, by using structuring methods to avoid detection. As described in the case study in the previous section, the defendants sent more than $1,000 to the P2P account associated with a self-proclaimed ISIS member.[81]

Cash

Cash remains a prevalent choice by terrorists around the world due to its anonymity, portability, and liquidity. Combined with the significant use of and demand for the U.S. dollar around the world, these factors have made U.S. currency specifically an attractive means of moving and using funds for terrorist groups and their supporters. Cash transactions generally occur outside of formal financial institutions, limiting recordkeeping and reporting and reducing the visibility of law enforcement and financial institutions into the source, movement, and ultimate use of funds.

Cash may be smuggled across borders using cash couriers, and is often used in conjunction with other methods, such as registered or unregistered MSBs. Even as terrorists have sought to take advantage of more modern methods of moving funds, they have continued to rely on cash. However, in recent years cash has increasingly been combined with more technologically advanced methods of moving funds like digital assets, such as in the ISIS fundraising case discussed earlier.

Domestically, U.S. authorities have identified numerous instances of U.S.-based individuals looking to support a variety of terrorist groups with cash. DVEs or HVEs may seek to make purchases in cash in preparation for an attack to limit their financial footprint. As illustrated by a case mentioned in the ISIS section above, for U.S.-based FTFs who attempt to travel overseas to join a terrorist group, they often carry cash with them.

Digital Assets

Since the publication of the 2024 NTFRA, the digital asset ecosystem has grown substantially. For example, the number of transactions on public blockchains reached highs of $3.8 billion monthly in early 2025—a 96% increase year-over-year.[82] As part of this growth, around 2,000 firms in the United States are registered as of mid-2025 to provide financial services in digital assets, referred to as digital asset service providers (also known as Virtual Asset Service Providers, or VASPs). Additionally, other financial institutions, like banks, continue to evaluate and some have already started to launch digital asset-related products and services, including offering to custody digital assets, creating exchange traded products that track the price of digital assets, and issuing their own digital assets. While various terms are used by parts of the U.S. government and the private sector, this report uses the term digital asset to refer to any digital representation of value that is recorded on a distributed ledger, including, but not limited to, cryptocurrencies, digital tokens, and stablecoins.[83]

In the United States, digital asset service providers have AML/CFT obligations if they fall under the BSA definition of a financial institution, which includes banks, broker-dealers, mutual funds, MSBs, futures commission merchants (FCMs), introducing brokers, and other forms of financial institutions.[84] Most of the more than 2,000 digital asset service providers in the United States are registered as MSBs, but depending on the activities in which the service provider engages, they may be considered financial institutions such as FCMs or securities intermediaries such as broker-dealers. Each of these types of financial institutions has AML/CFT obligations, including requirements to

81 Id.

82 White House, "Strengthening American Leadership in Digital Financial Technology" (Jul. 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

83 For the purpose of consistency, this terminology is also used in case examples, but this is intended only to facilitate an understanding of illicit finance risk and does not alter any existing legal obligations and does not create or confer any legal rights, privileges, or benefits that may be enforced in any way by private parties.

84 FinCEN, "Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets," (Oct. 11, 2019), https://www.fincen.gov/sites/default/files/2019-10/CVC percent20Joint percent20Policy percent20Statement_508 percent20FINAL_0.pdf.

establish and implement an AML program[85] and recordkeeping and reporting requirements, including SAR filing obligations.[86]

The U.S. government assesses that both international terrorist and DVE groups have continued, and in some cases expanded, using digital assets to generate and transfer funds. Certain groups, like ISIS and Hamas, use digital assets more commonly than other groups. In particular, Treasury observed a notable increase in 2024 in ISIS's use of digital assets for organizational transfers and donations from international supporters; additionally, as explained above, digital assets are a common method used by U.S.-based persons to send funds to ISIS.[87] Additionally, while Hamas announced in 2023 that it would stop accepting Bitcoin payments, the group continues to solicit donations in other digital assets.[88] Still, the U.S. government assesses that terrorists continue to prefer traditional financial products and services. This preference is likely due to the price volatility of many digital assets, the limited ability to purchase goods and services with digital assets, and a lack of infrastructure necessary to exchange digital assets for fiat currency in some jurisdictions where terrorist groups operate.

In line with the 2024 NTFRA, terrorist groups continue to use stablecoins—digital assets designed to maintain a stable value relative to a national currency or other reference assets—for donations and funds transfers. Stablecoins purport to be less volatile than other digital assets and may enable terrorist groups to utilize digital assets while mitigating the financial risks associated with price fluctuations. Additionally, stablecoins may be preferred by digital asset service providers (i.e., VASPs) used by terrorists to exchange digital assets for fiat currency. In particular, terrorist groups demonstrate a preference for U.S. dollar-denominated stablecoins, perhaps due to price stability, availability, or liquidity.[89]

Consistent with the 2024 NTFRA, most cases of terrorists using digital assets involve groups fundraising online and specifically soliciting digital assets from donors, often as one type of donation option. Such fundraising campaigns are often disseminated through social media or encrypted apps like Telegram and often solicit funds in digital assets and fiat currency, enabling the donor to decide which method to use. Individual donors can send digital assets from a digital asset service provider or an unhosted digital asset wallet[90] to a digital asset address owned by the terrorist group, although the group may attempt to obscure its ownership of the wallet address. For example, Hamas claims to change wallet addresses for each donation to prevent identification and attribution of Hamas and donor wallet addresses.[91] Some terrorist groups, like ISIS-K, have also solicited donations in anonymity-enhanced cryptocurrencies to further obfuscate the movement of funds.[92] Additionally, donors themselves may take precautions, including by using a virtual private network (VPN).[93]

---

85 See 31 C.F.R. § 1020.210 (banks); 31 C.F.R. § 1021.210 (casinos and card clubs); 31 C.F.R. § 1022.210 (MSBs); 31 C.F.R. § 1023.210 (brokers or dealers in securities); 31 C.F.R. § 1024.210 (mutual funds); 31 C.F.R. § 1026.210 (futures commission merchants and introducing brokers in commodities).

86 See 31 C.F.R. § 1020.320 (banks); 31 C.F.R. § 1021.320 (casinos and card clubs); 31 C.F.R. § 1022.320 (MSBs), 31 C.F.R. § 1023.320 (brokers or dealers in securities), 31 C.F.R. § 1024.320 (mutual funds), and 31 C.F.R. § 1026.320 (futures commission merchants and introducing brokers in commodities). A suspicious transaction must be reported if it is conducted or attempted by, at, or through the financial institution and the amount involved exceeds a certain threshold.

87 Fact Sheet on ISIS Financing.

88 Department of Justice, "Justice Department Disrupts Hamas Terrorist Financing Scheme Through Seizure of Cryptocurrency," (Mar. 27, 2025), https://www.justice.gov/opa/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure-cryptocurrency.

89 For more details, please see the 2024 NTFRA, p. 20 and the 2025 FinCEN ISIS Advisory (FinCEN, "FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates," Apr. 1, 2025 https://www.fincen.gov/system/files/advisory/2025-04-01/FinCEN-Advisory-ISIS-508C.pdf).

90 Unhosted wallets enable users to retain custody of their digital assets and transfer them without the involvement of a financial institution.

91 See Seizure Warrant, USA v. In the Matter of the Seizure of All Virtual Currency Stored Within, or Associated With, the Virtual Currency Addresses and Accounts in the Custody of Two Virtual Asset Service Providers, Case No. 25-sz-20, D.D.C. (Mar. 25, 2025), p. 22.

92 For more details, please see FinCEN, "FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates," Apr. 1, 2025 https://www.fincen.gov/system/files/advisory/2025-04-01/FinCEN-Advisory-ISIS-508C.pdf).

93 Department of Justice, "Detroit Man Pleads Guilty to Concealing His Cryptocurrency Donations to ISIS." (Jul. 8, 2025), https://www.justice.gov/usao-edmi/pr/detroit-man-pleads-guilty-concealing-his-cryptocurrency-donations-isis.

For example, in July 2025, Jibreel Pratt pleaded guilty to two counts of concealing digital assets donations he intended to make to ISIS.[94] In February 2023, Pratt initiated a conversation with a confidential human source (CHS) who Pratt believed was an ISIS member who could facilitate overseas travel to join ISIS. In March and May 2023, Pratt sent Bitcoin to the CHS, intending that the money would be used to help pay for the travel of other individuals who were purportedly traveling to join ISIS and/or to help fund an individual who Pratt believed would commit an act of violence in support of ISIS. Pratt concealed the nature and source of his Bitcoin transfers by using a privacy focused VPN and an app that encrypted private keys and transaction data.

Terrorist groups and their donors may use other techniques to obfuscate the movement of donated funds and the identity of donors themselves, including the use of digital asset service providers incorporated or based outside of the United States in jurisdictions with weak or non-existent AML/CFT controls.[95] In the Hamas case study noted earlier, the group directed donors to use certain digital asset service providers to transfer digital assets to the terrorist group's wallet address. In a second case noted in the ISIS section above, the donor sent digital assets to Türkiye, where they were smuggled to ISIS members in Syria, including by being converted into fiat currency and secretly passed to the intended recipients.[96]

In addition to using digital assets for donations, terrorist groups may also use digital assets to make funds transfers or to support terrorist attacks. In particular, ISIS uses digital assets to transfer funds within various entities including ISIS Core and al-Siddiq Office, and ISIS-K partially funded the terrorist attack on Crocus Hall in Moscow using digital assets.[97] In addition, ISIS and other terrorist groups may prefer to use digital assets due to the ability to move remaining funds quickly on the blockchain after potential arrests, seizures, or other disruptions by law enforcement that threaten their financing networks.

To conduct transfers and receive donations, terrorist groups may use financing networks across several jurisdictions to move digital assets. These networks use several different exchanges, sometimes even transferring assets within accounts at the exchanges, as well as unhosted wallets to hide both the origin and the final destination of funds. Since fiat currency is often most useful in the ultimate financing of terrorist activity, financiers may seek to cash out the digital assets by using exchanges or over-the-counter brokers, especially those located in jurisdictions with weak compliance regimes, after applying obfuscation techniques. Groups may also use donated and transferred digital assets for a variety of purposes, including the procurement of weapons, propaganda creation or dissemination, logistics, or planning a specific act of violence, although purchasing goods and services often requires exchanging digital assets for fiat currency.

Non-Profit Organizations (NPOs)

The United States has long recognized the importance of the NPO sector. Charitable organizations provide essential humanitarian aid and other assistance to vulnerable populations, perform other important services for the public good, and build communities across the world. While malign actors have historically exploited and continue to exploit certain aspects of the NPO sector to raise funds, today, the vast majority of U.S.-based NPOs face little exposure to TF.

This is the result of a variety of factors, including concerted efforts by international standard setting bodies to modernize AML/CFT standards and best practices to protect NPOs from TF abuse, the United States' risk-based approach to oversight of NPOs as well as the decades-long partnerships between the U.S. government, the NPO sector, financial institutions, and the donor community. Additionally, in the last decade, the charitable sector has

94 Id.

95 See Seizure Warrant, USA v. In the Matter of the Seizure of All Virtual Currency Stored Within, or Associated With, the Virtual Currency Addresses and Accounts in the Custody of Two Virtual Asset Service Providers, pp. 22-23, 26; Indictment, USA v. Besciokov, et al, Case No. 1:25-cr-00039, E.D.Va. (February 27, 2025), p. 9, para 18(b).

96 Department of Justice, "Man Sentenced to Over 30 Years in Prison for Crypto-Terror Financing Scheme," (May 8, 2024), https://www.justice.gov/opa/pr/man-sentenced-over-30-years-prison-crypto-terror-financing-scheme.

97 See e.g., Fact Sheet on ISIS Financing.

made important strides in addressing and mitigating TF threats through implementing internationally recognized best practices on due diligence measures and risk mitigation efforts, often in collaboration with Treasury and the broader U.S. government. The U.S. government, working with financial institutions, has also prioritized protecting NPOs' access to the regulated financial system to conduct legitimate charitable activities, resulting in greater transparency and less reliance on the utilization of alternative financial channels.

The United States' Risk-Based Approach to NPO Oversight

The United States adopts a multifaceted, whole-of-government approach to conducting oversight of a large and diverse charitable sector for TF risks. The United States applies focused, proportionate, and risk-based mitigation measures to NPOs in line with their TF risk. These measures are informed through sustained private-sector engagements and a dialogue between policymakers, regulators, financial institutions and the NPO community to ensure that the legitimate provision of aid is protected and to the greatest extent possible, flows through supervised channels. Through this whole-of-government approach, the United States is able to identify and appropriately address cases of charities being misused by terrorist groups to prevent this behavior and deprive terrorists of their funds. This approach also prioritizes the protection of humanitarian channels, including the provision of assistance and aid.

Treasury continues to see cases of foreign NPOs being created or abused for TF purposes and has utilized its sanctions authorities to protect the international financial system and the NPO sector from those actors. When cases do arise, U.S. authorities will utilize all tools at their disposal to address violations. As an example, in 2024, federal prosecutors charged a Syrian national for diverting $9 million in humanitarian assistance provided by the U.S. Agency for International Development (USAID) to a Syria-based NGO, intended for Syrian civilians, to armed groups like Al-Nusrah Front (the AQ affiliate in Syria at the time).[98]

Financial Access Work and Sustained Outreach

The United States recognizes the importance of encouraging NPOs to conduct transactions via regulated financial and payment channels, where feasible. Treasury has undertaken substantial efforts to reduce the incentives of NPOs to use cash and to increase their incentives to keep transactions within the regulated financial sector where appropriate through a variety of measures. Treasury also reiterates the importance of financial institutions adopting risk-based AML/CFT and sanctions controls to ensure charitable NPOs' continued access to the financial system.

As noted in previous NTFRAs, Illicit Finance Strategies, and Treasury's De-risking Strategy, the U.S. government prioritizes encouraging and underscoring the importance of NPOs having access to and conducting transactions through the formal financial system, noting that the alternative increases the risk of TF threats to the sector. Additionally, the U.S. government has also prioritized efforts to standardize humanitarian assistance-related carveouts across U.S. sanctions regimes and those at the UN to facilitate humanitarian-related activity and mitigate potential unintended consequences of new U.S. sanctions programs. The availability of general licenses within OFAC's sanctions programs ensures that NPOs can retain access to the financial system to process transactions in service of their operations, including life-saving services in jurisdictions where there is an increased risk of terrorist financing. Moreover, Treasury has provided guidance to financial institutions on how to implement a risk-based approach to banking NPO customers without placing undue burden on the financial institutions.

Today, the vast majority of U.S. charitable NPOs face little exposure to TF with only a small subset of charitable NPOs with an international presence at risk for TF. Where the U.S. government does assess higher TF risk stems from the nexus between U.S.-based NPOs and foreign NPOs in jurisdictions with less effective AML/CFT controls. Failure to adopt appropriate risk mitigation measures to guard against unwitting diversion when operating in conflict zones where terrorist groups are active can increase TF vulnerability. Non-U.S. NPOs based in jurisdictions with less effective AML/CFT controls are more at risk of TF abuse, according to their types, activities, or characteristics.

98 Department of Justice, "Syrian National Charged with Diverting $9 Million in U.S.-funded Humanitarian Assistance to a Terrorist Organization Affiliated with Al-Qaida," (Nov. 19, 2024), https://www.justice.gov/usao-dc/pr/syrian-national-charged-diverting-9-million-us-funded-humanitarian-assistance-terrorist.

Additionally, as noted in previous NTFRAs, the U.S. government continues to see the prevalence of foreign-based sham charities and fraudulent fundraising efforts as a cover to raise funds. For example, fraudulent charitable appeals with no connection to registered NPOs continue to be a common typology used by terrorist groups. This allows terrorist organizations to cast wide nets to raise funds through social media or crowdfunding websites making it difficult for unwitting individuals to detect the connection to TF. Other fact patterns include terrorist organizations setting up sham charities in foreign jurisdictions with weak AML/CFT controls allowing for funds to be raised under the guise of providing humanitarian assistance but instead funneling money to terrorist activities or causes. However, Treasury notes that TF risks and fact patterns involving these sham charities and foreign-based NPOs are distinct from legitimate U.S. NPOs, registered in the United States. Treasury is focused on identifying and designating sham charitable organizations, which reduces the overall TF risk of the NPO sector.

- In June 2025, Treasury disrupted a sham overseas charity network funding the terrorist organizations Hamas and the Popular Front for the Liberation of Palestine (PFLP). Specifically, OFAC designated five individuals and five sham charities located abroad that are prominent financial supporters of Hamas's Military Wing and its terrorist activities and are responsible for funding Hamas's Military Wing under the pretense of conducting humanitarian work, both internationally and in Gaza.[99] This action highlighted Hamas and the PFLP's longstanding abuse of the trust of the international community and public support for legitimate humanitarian causes to fund terrorist activities and bring violence to the Israeli and Palestinian people.
- In October 2024, in a joint action with Canada, Treasury designated the Samidoun Palestinian Prisoner Solidarity Network, or "Samidoun," a sham charity that serves as an international fundraiser for the PFLP terrorist organization. The PFLP uses Samidoun to maintain fundraising operations in both Europe and North America. At the same time, Treasury also designated Khaled Barakat, a member of the PFLP's leadership. Together, Samidoun and Barakat play critical roles in external fundraising for the PFLP.[100]

CONCLUSION

Since the publication of the 2024 NTFRA, terrorist groups at large have continued to demonstrate resilience in the face of continued military and financial pressures, and have adapted —and taken advantage of—the evolving global geopolitical landscape. The United States continues to face a broad spectrum of terrorist threats from an ideologically diverse set of actors who maintain the capability and will to attack the U.S. homeland, U.S. personnel, and U.S. interests abroad. FTOs persist in spreading their propaganda online to radicalize individuals in the United States, motivating acts of violence and the provision of financial or material support in service of their extremist ideologies. DVEs have also continued to threaten the United States, and combatting the financing of lone attacks by DVE and HVE actors remains a top challenge for U.S. government authorities. Further, the continued campaign of violence from international drug cartels has necessitated the USG to use new tools to protect the United States, including the designation of certain cartels as FTOs, as part of the government-wide policy to pursue the total elimination of these organizations' presence in the country.

Sustained U.S. counterterrorism efforts have made the world demonstrably safer, with U.S. leadership in combatting TF serving as a cornerstone of these successes. As terrorists continue to seek out new ways to reliably raise, move, and use funds for their heinous purposes, now more than ever combatting TF is a national security imperative. As terrorist financing methods evolve, the U.S. Government must remain agile and proactive in strengthening its tools, authorities, and partnerships to disrupt these networks and deny terrorists the financial resources they rely on to carry out attacks against innocent civilians.

99 Department of Treasury" not "Treasury, "Treasury Disrupts Sham Overseas Charity Networks Funding Hamas and the PFLP," (Jun. 10, 2025), https://home.treasury.gov/news/press-releases/sb0162.

100 Department of Treasury, "United States and Canada Target Key International Fundraiser for Foreign Terrorist Organization PFLP," (Oct. 15, 2024), https://home.treasury.gov/news/press-releases/jy2646.

METHODOLOGY AND TERMINOLOGY

The terminology and methodology of the 2026 NTFRA are based on the guidance of the Financial Action Task Force (FATF), which is the international standard-setting body for AML/CFT safeguards. This guidance lays out a process for conducting a TF risk assessment at the national level.[101] The underlying concepts for this risk assessment are threats, vulnerabilities, consequences, and risk. This approach uses the following key concepts:

- *Threat*: A threat is a person, a group of people, or an activity with the potential to cause harm by raising, moving, storing, or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. In the TF context, this includes terrorist groups and their facilitators, as well as radicalized individuals seeking to exploit the U.S financial system to raise, move, and use funds.
- *Vulnerability*: A vulnerability can be exploited to facilitate TF, both in the raising of funds for terrorist networks and the movement of funds to terrorists and terrorist organizations. It may relate to a specific financial product used to move funds or a weakness in regulation, supervision, or enforcement or reflect unique circumstances that may impact opportunities for terrorist financiers to raise or move funds or other assets. There may be some overlap in the vulnerabilities exploited for both money laundering (ML) and TF.
- *Consequence*: Consequence refers to the impact or harm that a TF threat may cause if it can exploit a vulnerability and be operationalized. Not all TF methods have equal consequences. The methods that raise or move the greatest amount of money most effectively often present the greatest potential TF consequences. However, it may require only a small amount of funds to execute a terrorist act with devastating human consequences. Therefore the 2026 NTFRA focuses on threats and vulnerabilities in determining TF risks.
- *Risk*: Risk is a function of threat, vulnerability, and consequence.

The 2026 NTFRA relies on an analysis of criminal prosecutions, Treasury designations, financial institution reporting, threat assessments and advisories, and other information available to the U.S. government, along with a review of information on TF from international bodies such as the Financial Action Task Force (FATF) and nongovernmental organizations (NGOs). This information was used to determine (1) the terrorist groups or movements that are most active in raising and moving funds through the United States and the U.S. financial system, and the methods and typologies used by those groups to raise and move funds, (2) which characteristics of financial products, services, or market participants facilitate the raising or movement of funds by or on behalf of terrorists or terrorist organizations, and (3) the extent to which domestic laws and regulations, law enforcement investigations and prosecutions, regulatory compliance and supervision, enforcement activity, and international outreach and coordination mitigate identified TF threats and vulnerabilities. This research and analysis was then used to identify the resulting TF risks facing the United States. Data collected is current as of January 31, 2026.

101 FATF, Terrorist Financing Risk Assessment Guidance, (Jul. 2019), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.

PARTICIPANTS

In drafting this assessment, the Department of the Treasury's Office of Terrorist Financing and Financial Crimes consulted with staff from the following U.S. government agencies, who also reviewed this report:

- **U.S. Department of the Treasury**
  - Office of Terrorism and Financial Intelligence
    - Financial Crimes Enforcement Network (FinCEN)
    - Office of Foreign Assets Control (OFAC)
    - Office of Intelligence and Analysis (OIA)
    - Office of Terrorist Financing and Financial Crimes (TFFC)
  - Internal Revenue Service (IRS)
    - Criminal Investigation (CI)
    - Tax Exempt & Government Entities Division (TEGE)
- **U.S. Department of Justice (DOJ)**
  - Criminal Division
  - National Security Division
  - Federal Bureau of Investigation (FBI)
    - Counterterrorism Division
    - Criminal Investigative Division
- **U.S. Department of State**
  - Bureau of Counterterrorism
  - Bureau of Economics, Energy, and Business
- **National Counterterrorism Center (NCTC)**
- **Staff of the Federal Functional Regulators**[102]

102 This consists of staff of the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC).

LIST OF ACRONYMS

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
AQ	al-Qa'ida
BSA	Bank Secrecy Act
CBDC	Central Bank Digital Currency
CHS	Confidential Human Source
CFTC	Commodity Futures Trading Commission
CVC	Convertible Virtual Currency
DHS	U.S. Department of Homeland Security
DVE	Domestic Violent Extremist
FATF	Financial Action Task Force
FCM	Futures Commission Merchant
FTO	Foreign Terrorist Organization
HVE	Homegrown Violent Extremist
IC	Intelligence Community
IJO	Islamic Jihad Organization
IRGC	Islamic Revolutionary Guard Corps
ISIS	Islamic State of Iraq and Syria
ISIS-DRC	ISIS- Democratic Republic of the Congo
ISIS-K	ISIS-Khorasan
MSB	Money Services Business
NGO	Non-Governmental Organization
NMLRA	National Money Laundering Risk Assessment
NPFRA	National Proliferation Financing Risk Assessment
NTFRA	National Terrorist Financing Risk Assessment
NPO	Non-Profit Organization
NPRM	Notice of Proposed Rule Making
ODNI	Office of the Director of National Intelligence
P2P	Peer-To-Peer
PFLP	Popular Front for the Liberation of Palestine
SAR	Suspicious Activity Report
SDGT	Specially Designated Global Terrorist
TF	Terrorist Financing
UAE	United Arab Emirates
UN	United Nations
USAID	U.S. Agency for International Development
VA	Virtual Asset
VASP	Virtual Asset Service Provider


THE DEPARTMENT OF THE TREASURY
1789