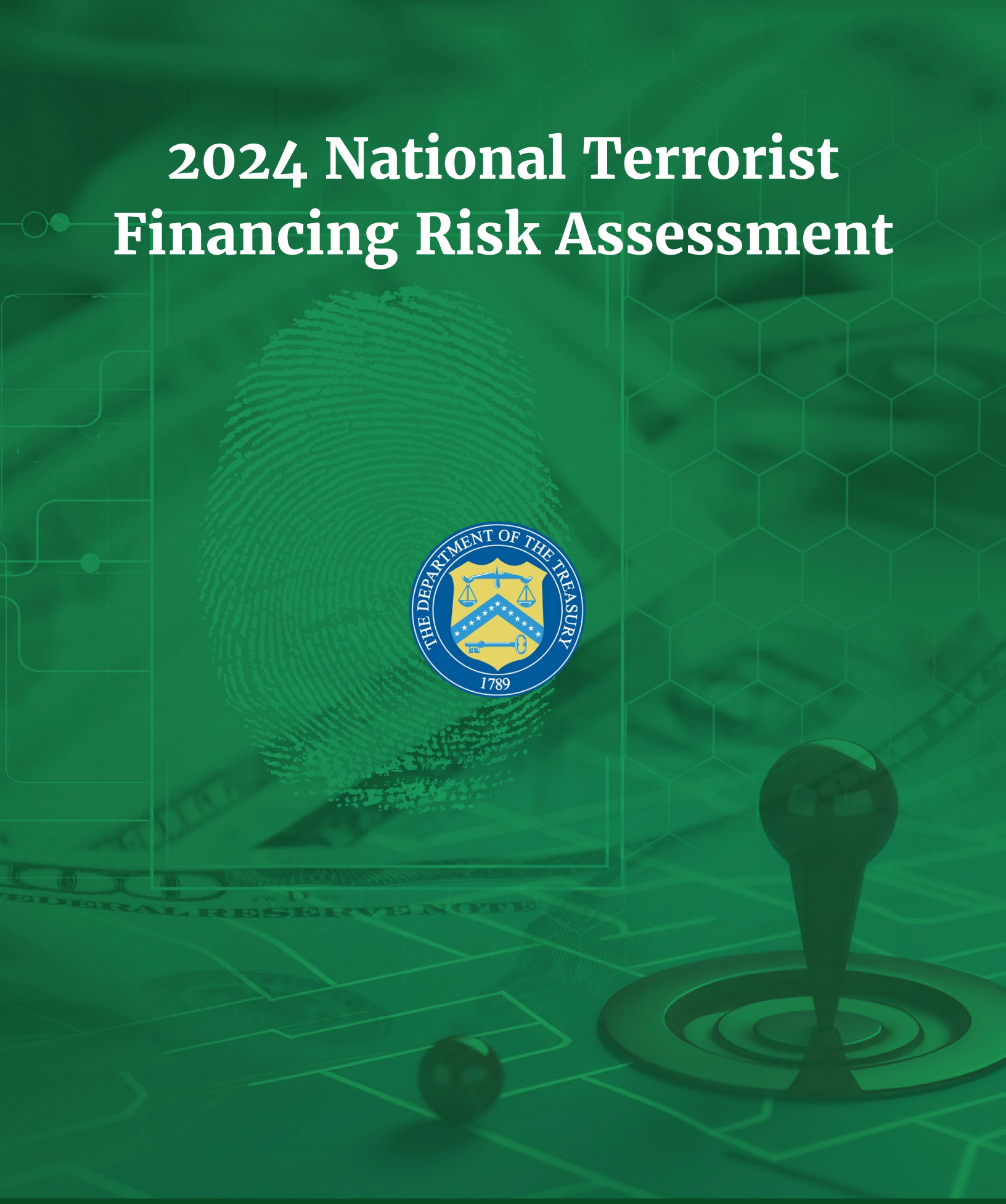
2024 National Terrorist Financing Risk Assessment



February 2024

Department of the Treasury

2024 National Terrorist Financing Risk Assessment

Table of Contents

EXECUTIVE SUMMARY

Over the past 20 years, the terrorist threat to the United States has evolved significantly. In that time, our counterterrorism and counter-terrorist financing (CTF) posture has evolved alongside the threat, taking the lessons learned from the immediate aftermath of 9/11 and applying them to new threat actors and terrorist financing (TF) methods.

This 2024 National Terrorist Financing Risk Assessment (NTFRA) comes almost 10 years after the Department of the Treasury (Treasury) published the inaugural NTFRA in 2015. At that time, terrorism was the primary national security threat to the United States, and Al-Qa'ida (AQ) and its affiliates were the primary terrorism threat to the United States. The Islamic State of Iraq and Syria (ISIS) was quickly growing in both size and its use of extreme violence in Iraq and Syria. The United States faced regional terrorism threats from other Sunni jihadist groups in Afghanistan and Pakistan, Southeast Asia, and East Africa. Within the United States, there was a smaller but growing risk of individuals, often referred to as lone wolf terrorists, who were inspired by, but unaffiliated with, foreign terrorist groups and carrying out low-cost attacks using firearms, vehicles, or homemade explosives. Hizballah and other Iranian-backed groups also continued to threaten U.S. foreign interests around the world. While some of these groups relied on Iran, the world's foremost state sponsor of terrorism, for financial support, others sought funds through kidnapping for ransom or other criminal activity or by exploiting charitable organizations or causes to raise funds. These funds moved primarily through money transmitters (registered and unregistered), banks (where functioning banking systems existed), and cash.

Almost 10 years later, the United States faces a much more complex international security environment in which terrorism is still the greatest threat to the homeland but several other major security threats also exist.[1] Russia and the People's Republic of China seek to undermine or create alternatives to the U.S.-led rules-based global order. Other shared international challenges, including humanitarian crises, international health concerns, and rapidly emerging or evolving technologies with the potential to disrupt traditional business and society, are increasingly intertwined with broader national security risks. These trends all impact the current terrorism landscape.

Today, the primary terrorism threat to the homeland comes from individuals in the United States who are inspired by AQ, ISIS, or domestic violent extremist (DVE) ideologies and who seek to carry out deadly attacks without direction from a terrorist group.[2,3] These individuals may be radicalized to violence online through social media and can carry out these attacks with limited warning.

In particular, DVE movements, motivated by racial bias, grievances against authority, or a mix of these and other ideologies, have metastasized over the last decade to become one of the most serious terrorism threats facing the United States, particularly racially and ethnically motivated

1 Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, p. 22-24, (Feb. 6, 2023) (ODNI 2023 Annual Threat Assessment).

2 Federal Bureau of Investigation and Department of Homeland Security, "Strategic Intelligence Assessment and Data on Domestic Terrorism", (Oct. 2022), https://www.dhs.gov/sites/default/files/2022-10/22_1025_strategic-intelligence-assessment-data-domestic-terrorism.pdf, (FBI/DHS Intel Assessment on DT).

3 Individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences—some of which include racial or ethnic bias, or strong anti-government or anti-authority sentiments—are described as domestic violent extremists (DVEs), whereas homegrown violent extremists (HVEs) are individuals inspired primarily by foreign violent jihadist beliefs. HVEs are individuals inspired primarily by foreign terrorist groups, but who are not receiving individualized direction from those groups.

violent extremists (RMVE).[4] The last several years have witnessed the emergence of these networks of individuals in the United States who seek to carry out violent attacks against minorities, government authorities, or critical infrastructure.[5]

At the same time, foreign terrorist threats to the United States and U.S. interests persist. The primary threat to the United States overseas comes from ISIS-inspired affiliates that seek to attack the United States, its citizens, and its interests. AQ remains committed to attacking U.S. interests, although the threat is greatest in the regions where its affiliates operate rather than in the U.S. homeland. More recently, the October 2023 terrorist attacks by Hamas against Israel serve as a stark reminder that though much headway has been made in the fight against terrorism, this threat is close at hand. Numerous terrorist groups have called for or threatened attacks on U.S. soil and against U.S. interests abroad since those events. The Hamas attack and subsequent attacks by Hizballah, Palestinian Islamic Jihad (PIJ), and other Iran-affiliated militias[6] showed both the reach of Iran's terrorist proxies to threaten U.S. personnel and allies and how quickly a terrorism threat to the United States and its interests overseas can reemerge.

As the nature of the terrorist threat and the actors involved have grown more varied, terrorist financing in the United States has similarly evolved over the past decade. While some individuals still seek to send money to foreign terrorist groups, many now forgo "financial jihad" and instead focus their efforts (and resources) on attacks on unprotected civilian targets in the United States. ISIS and AQ-related financial activity in the United States is most commonly associated with U.S. persons aspiring to travel abroad to conflict zones or attempting to send money to these groups or affiliates. Funds used to support travel-related activity have primarily been generated from legitimate activities, and cash is often used for these purposes. In some instances, U.S.-based individuals have sought to fundraise extensively or solicited funds specifically for ISIS.

Hizballah continues to utilize the formal and informal U.S. financial system, permissive jurisdictions, as well as sophisticated financial schemes to launder, raise, and move funds. Additionally, as more information regarding the financing of Hamas comes to light after the October 2023 terrorist attacks, it is clear that the group looks to the United States as a venue for generating revenue, casting a large net with diverse methods and sources of fundraising.

While terrorists continue to experiment and adapt to changes in technology, they still utilize tried-and-true methods. Banks and money transmitters are still exploited for their reach and capacity to send large volumes, but some terrorist groups have also increased their capability and understanding of using virtual assets to transfer funds; some groups have also begun experimenting with alternative types of virtual assets. Typologies of TF involving the charitable sector have also shifted from abuse of legitimate charities to sham charities and fraudulent charitable appeals. Lastly, the internet has facilitated a range of nefarious financial activity, and numerous terrorist groups have been observed utilizing crowdfunding and various methods of online fundraising to raise funds from witting and unwitting donors.

4 See Testimony of FBI Director Christopher Wray, Worldwide Threats to the Homeland, (Nov. 15, 2023) (FBI 2023 Threats Testimony).

5 Importantly, this risk assessment does not evaluate the actions of individuals engaged solely in activities protected by the First Amendment or other rights secured by the U.S. Constitution.

6 Congressional Research Service, Israel and Hamas October 2023 Conflict: Frequently Asked Questions (FAQs), p.37-38, (Oct. 2023), https://crsreports.congress.gov/product/pdf/R/R47754.

Introduction

The 2024 NTFRA identifies the TF threats, vulnerabilities, and risks the United States faces, updating the 2022 NTFRA.[7] This report, as well as the 2024 National Money Laundering Risk Assessment (NMLRA) and 2024 National Proliferation Financing Risk Assessment (NPFRA), provide an overview of the current illicit finance risks to the United States. These risk assessments also inform and complement the Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (Priorities) issued by the Financial Crimes Enforcement Network (FinCEN).[8] These Priorities include both international and domestic terrorist financing risks. This assessment was prepared according to Sections 261 and 262 of Countering America's Adversaries through Sanctions Act (P.L. 115-44) as amended by Section 6506 of the Fiscal Year 2022 National Defense Authorization Act (P.L. 117-81).

Relevant component agencies, bureaus, and offices of Treasury, the Department of Justice (DOJ), federal financial regulators, and other government agencies participated in developing the risk assessment. The 2024 NTFRA is based on an analysis of criminal prosecutions[9], discussions with relevant authorities and private sector entities, a review of government actions and analysis, including Treasury designations and private sector research issued since the 2022 NTFRA.[10]

7 The 2022 NTFRA is available at 2022 National Terrorist Financing Risk Assessment (treasury.gov).

8 See https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

9 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.

10 The review period is from January 1, 2022, to December 31, 2023.

THREATS

Domestic Violent Extremism and Transnational Racially or Ethnically Motivated Violent Extremism

Domestic Violent Extremism

Law enforcement agencies have stated that the threat posed by DVEs[11] is one of the most pressing terrorism threats to the United States.[12] A DVE is an individual based and operating primarily in the United States, without direction or inspiration from a foreign terrorist group or other foreign power, who seeks to further political or social goals wholly or in part through unlawful acts of force or violence.[13] The U.S. government uses the following five categories, based on ideological motivations, to group DVE actors: (1) racially or ethnically motivated violent extremists (RMVE); (2) anti-government or anti-authority violent extremists (AGAAVE) (including militia violent extremists (MVE)); (3) animal rights or environmental violent extremists; (4) abortion-related violent extremists; and (5) other DVE threats that do not fall into the prior four categories.[14]

Domestic terrorism investigations have more than doubled since 2020, according to the Federal Bureau of Investigation (FBI).[15] The U.S. Intelligence Community (IC) has assessed that the DVE threat is fueled by a range of ideological and sociopolitical grievances, exacerbated by galvanizing issues such as perceived election fraud, the COVID-19 pandemic, and immigration policy, among other issues, and this threat will continue to persist for the foreseeable future.[16]

The most concerning threat categories of DVE are RMVE actors, particularly those driven by a belief in the superiority of the white race, as discussed in more detail in the next section. RMVEs pose the most consistent threat of lethal and non-lethal violence against religious, cultural, and government targets.[17,18] Threats have also increased in the past two years from AGAAVEs, including those motivated by a desire to commit violence against individuals or entities they perceive to be associated with a specific political party or faction thereof.[19]

In recent years, U.S. government personnel, including military and law enforcement, have increasingly become a target of DVEs, especially by MVE actors.[20] In addition, DVEs have increasingly called for

11 Some entities use the terms DVE and Domestic Terrorism (DT) interchangeably, but consistent with law enforcement, this assessment will use DVE as the label for an individual or group until a violent or terrorist act is committed, and then use DT after that point.

12 FBI/DHS Intel Assessment on DT, p. 2.

13 Office of the Director of National Intelligence, *Domestic Violent Extremism Poses Heightened Threat in 2021*, p. 3 (Mar. 1, 2021) (ODNI DVE Assessment).

14 Federal Bureau of Investigation, "Domestic Terrorism: Definitions, Terminology, and Methodology", p. 2 (Nov. 2020), https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf/view.

15 FBI 2023 Threat Testimony.

16 ODNI DVE Assessment, p. 2, FBI/DHS Intel Assessment on DT, p.37.

17 FBI/DHS Intel Assessment on DT, p. 6.

18 In May 2023, DHS named these as the targets: "US critical infrastructure, faith-based institutions, individuals or events associated with the LGBTQIA+ community, schools, racial and ethnic minorities, and government facilities and personnel, including law enforcement." See https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-24-2023.

19 Id.

20 FBI/DHS Intel Assessment on DT, pp. 37, 40.

physical attacks on critical infrastructure. DVEs, particularly RMVEs promoting accelerationism—an ideology that seeks to destabilize society and trigger a race war—have encouraged mobilization against lifeline and other critical functions, including attacks against the energy, communications, and public health sectors.[21]

- In February 2023, two individuals were charged federally with conspiracy to destroy an energy facility. From at least June 2022 to the present, one of the defendants conspired to carry out attacks against critical infrastructure, specifically electrical substations, in furtherance of his racially or ethnically motivated violent extremist beliefs. The second defendant collaborated on a plan to carry out the attacks.
- In April 2023, two individuals were sentenced for conspiring to provide material support to terrorists, with a third co-conspirator previously pleading guilty in February 2022.[22] As part of the conspiracy, each defendant was assigned a substation in a different region of the United States. The plan was to attack the substations, or power grids, with powerful rifles. The defendants believed their plan would cost the government millions of dollars and cause unrest for Americans in the region. They had conversations about how the possibility of the power being out for many months could cause war, even a race war, and induce the next Great Depression.

For most DVE attacks, the predominant means of funding is self-financing.[23] These funds generally come through legal means, such as personal savings or earned income. In some cases, radicalized individuals engage in legitimate commercial activity, like selling t-shirts or other merchandise, to raise funds for certain groups. Other DVEs have sought to profit from illicit activity such as drug trafficking.[24] DVEs have also used online forums and crowdfunding websites to solicit donations from other people, often for activities like legal fees or travel to training camps or protests, much of which is constitutionally protected. Some DVEs have solicited or transferred funds in virtual assets or expressed interest in using virtual assets to move funds pseudonymously.[25]

Many DVEs and those supporting them have a sophisticated understanding of what conduct (financial or otherwise) is permissible versus illegal, making it challenging to link financial activity with violent conduct. Further, the fact that most DVE attacks are self-funded through legitimate sources means that associated transactions may not appear suspicious, making it difficult for financial institutions to identify associated transactions prior to an attack. This limits financial institutions' ability to identify and notify law enforcement pre-emptively about a given individual who may be linked to acts of violence.[26]

21 Department of Homeland Security, *Homeland Threat Assessment 2024*, p.18 (Sep. 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf.

22 Office of Public Affairs, "Two Men Sentenced for Conspiring to Provide Material Support to Plot to Attack Power Grids in the United States," U.S. Department of Justice, (April 21, 2023), https://www.justice.gov/opa/pr/two-men-sentenced-conspiring-provide-material-support-plot-attack-power-grids-united-states.

23 United States Government Accountability Office, *Violent Extremism: Agencies' and Financial Institutions' Efforts to Link Financing to Domestic Threats*, p. 8, 10, (Sept.2023), (GAO Violent Extremism Report), https://www.gao.gov/assets/gao-23-105928.pdf.

24 Id.

25 Department of the Treasury, Treasury Roundtable on Domestic Violent Extremist Use of Virtual Currency and Launch of DVE Financing Resource Page, (Apr. 21, 2023), https://home.treasury.gov/news/press-releases/jy1433.

26 GAO Violent Extremism Report, p. 2, 8.

Transnational Racially or Ethnically Motivated Violent Extremism

According to an assessment by the Office of the Director of National Intelligence (ODNI), "transnational RMVEs continue to pose the most lethal threat to U.S. persons and interests, and a significant threat to U.S. allies and partners through attacks and propaganda that espouses violence."[27] RMVEs' ideologies, especially those involving white supremacy or neo-Nazism, often transcend domestic boundaries as the ideology itself is shared by other individuals and groups around the world.[28] Transnational RMVEs have had some contact with individuals and like-minded movements within the United States. The FBI assesses that in the United States, those advocating for white supremacy are the most likely subcategory of RMVEs to have transnational connections with foreign extremists that espouse similar beliefs, including in Australia, South Africa, Canada and throughout Europe.[29,30] This contact often occurs online; decentralized, transnational networks of RMVEs have proliferated online in recent years. [31] Some U.S.-based RMVEs have traveled abroad to meet with like-minded individuals or groups.[32] Additionally, evidence suggests that some RMVE attacks abroad have inspired individuals in the United States to commit similar attacks. [33]

Russia's war against Ukraine has elevated the popular appeal and strengthened the international nexus of certain RMVE groups. The IC has noted that the Ukraine war could present RMVE groups with an opportunity to gain battlefield experience and military equipment.[34] In June 2022, Treasury's Office of Foreign Assets Control (OFAC) designated two key supporters of the Russian Imperial Movement (RIM), a white supremacist, ultranationalist, paramilitary organization based in Russia with transnational connections that has carried out acts of terrorism around the world.[35] In 2020, RIM became the first white supremacist RMVE group to be designated as a terrorist group by the U.S. State Department.[36] RIM has sought to exploit the Russian war in Ukraine for its own benefit, provided paramilitary-style training to ideologically aligned individuals in Europe, and has had contact with organizations in the United States on an informal basis.[37]

Financial connections between international RMVE groups and U.S.-based RMVEs with similar ideologies are tenuous so far. Crowdfunding websites have served as one nexus between U.S.-based RMVE actors and individuals located overseas, but there is no evidence to suggest any significant or

27 ODNI 2023 Annual Threat Assessment, p. 33.

28 Testimony of Dr. Joshua A. Geltzer, *Stepping Out of the Shadows: How Violent White Supremacists Have Used Technology to Pose a Transnational Threat*, (Sep. 20, 2019), (Testimony of Dr. Joshua Geltzer), https://docs.house.gov/meetings/GO/GO02/20190920/109977/HHRG-116-GO02-Wstate-GeltzerJ-20190920.pdf.

29 Id.

30 Statement for the Record of Acting State Department Coordinator for the Bureau of Counterterrorism John Godfrey, Racially and Ethnically Motivated Violent Extremism: The Transnational Threat, (Apr. 29, 2021). https://homeland.house.gov/imo/ media/doc/2021-04-29-IC-HRG-Testimony-Godfrey.pdf.

31 ODNI 2023 Annual Assessment, p. 33: "Terrorgram, a loosely connected network of channels on the messaging application Telegram, has circumvented multiple efforts to moderate content. Terrorgram serves as a transnational forum for RMVEs to share propaganda, exchange operational guidance, and valorize the perpetrators of previous terrorist attacks."

32 Id.

33 Testimony of Dr. Joshua Geltzer, p.2.

34 ODNI 2023 Annual Threat Assessment, p. 33.

35 Department of Treasury, OFAC, "U.S. Sanctions Members of Russian Violent Extremist Group", (Jun.15, 2022), https://home.treasury.gov/news/press-releases/jy0817.

36 RIM was also designated as a terrorist group by Canada in 2021.

37 Department of State, "United States Designates Russian Imperial Movement and Leaders as Global Terrorists", (Apr. 7, 2020), https://2017-2021.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists/.

large-scale financial connections between U.S. RMVEs and groups overseas.[38]

Islamic State of Iraq and Syria (ISIS)

According to the ODNI Threat Assessment for 2023, ISIS remains a threat both regionally and globally despite suffering significant setbacks from losses to key leadership figures in the past two years due to numerous operations against ISIS core[39] in Syria and Iraq.[40] In response to sustained international pressure on the group and the loss of leadership figures, ISIS has adopted a less hierarchical, looser structure of networked affiliate groups.[41] Though ISIS core strength has been somewhat diluted, certain branches operate with near autonomy and are highly operationally capable.[42] The IC deems the largest ISIS threat to the United States emanates from these ISIS branches, such as ISIS-Khorasan (ISIS-K), that have the ambition and capabilities to conduct attacks beyond the Central Asia region.[43]

Though ISIS maintained a strong presence in the Middle East and Afghanistan throughout 2022 and 2023, ISIS-affiliated groups in various countries within Africa play an increasingly prominent role in the group as a whole, both financially and operationally. ISIS branches continue to operate extensively throughout the African continent while exploiting regional instability, weak governance, and local conflicts and grievances. The State Department assessed that ISIS waged a "large-scale terrorism campaign," particularly in Cameroon, Chad, Niger, and Nigeria, where the porous borders near the Lake Chad region provide easy transit routes for local ISIS affiliates, as well as in Afghanistan.[44] The strongest and most capable ISIS affiliates in Africa are ISIS-West Africa, ISIS-Democratic Republic of Congo (ISIS-DRC), and ISIS-Somalia. Additionally, ISIS-K in Afghanistan remains an important and powerful affiliate due to its role as a regional hub, transferring hundreds of thousands of dollars to financial facilitators as well as providing personnel and weapons to support external operations.[45]

Sustained international pressure has resulted in diminished revenue and a loss of several key financial facilitators, such as Bilal al-Sudani, and has created financial challenges for the group, putting more pressure to raise funds.[46] ISIS core still has access to dwindling cash reserves in Iraq and Syria, estimated to be around $25 million in late 2022, down from $500 million at the height of the ISIS caliphate.[47] Reports indicate that ISIS core's revenue may be declining, resulting in occasional skipped

38 Financial Action Task Force, *Crowdfunding for Terrorist Financing*, p. 25, (Oct. 2023), (FATF Crowdfunding for TF Report), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

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

40 ODNI 2023 Annual Threat Assessment, p. 32.

41 UN Analytical Support and Sanctions Monitoring Team, *32nd Report of the Analytical Support and Sanctions Monitoring Team*, pp. 5, 12 (Jul. 25, 2023) (32nd UN MT Report), https://undocs.org/S/2023/549.

42 Id.

43 Statement for the Record by General Michael "Erik" Kurilla, (Mar. 13, 2023), https://www.armed-services.senate.gov/imo/media/doc/Kurilla_SASC_Posture_Final_141200March2023.pdf, p. 3; ODNI 2023 Annual Threat Assessment, p. 32.

44 Department of State, Country Reports on Terrorism 2021, p. 4, Country_Reports_2021_Complete_MASTER.no_maps-011323-Accessible.pdf (state.gov).

45 Department of Treasury, "Fact Sheet: Countering ISIS Financing", (Jun. 16, 2023), (CIFG Fact Sheet 2023), 2023.06.16-Fact-Sheet-on-Countering-ISIS-Financing.pdf (treasury.gov).

46 Department of Treasury, OFAC, "Treasury Designates Senior ISIS-Somalia Financier", (Jul. 27, 2023), https://home.treasury.gov/news/press-releases/jy1652.

47 Department of Treasury, "Fact Sheet: Countering ISIS Financing", (Nov. 18, 2022), (CIFG Fact Sheet 2022) 2023.06.16-Fact-Sheet-on-Countering-ISIS-Financing.pdf (treasury.gov).

payments for ISIS fighters and their families due to financing constraints.[48]

Aside from cash reserves, ISIS generates significant income through various illicit and criminal activities. Kidnapping for ransom and extortion provides significant amounts of money to the group, especially for key ISIS branches, such as ISIS-K and ISIS-Somalia. ISIS-Somalia has also become one of the most important branches for ISIS financially, as it generates significant revenue for the group through extortion of local businesses and financial institutions, some of which is then transferred and distributed to other ISIS branches and networks.[49] ISIS-Somalia, overseen by Al-Karrar office, has served as a financial and communication hub for the global ISIS enterprise, facilitating funds transfers to other branches and networks through mobile money platforms, cash transfers, hawala, and money laundering through businesses.[50]

Lastly, contributions from individual supporters also supplement the group's cash flows. ISIS has sought to aggressively fundraise online using social media, encrypted mobile applications, online gaming platforms, and virtual asset service providers (VASPs) for fund transfers.[51] ISIS facilitators have adapted to new technologies like virtual assets. For example, certain branches, such as ISIS-K, have increased their understanding of virtual assets. ISIS also seeks to raise money to free pro-ISIS sympathizers and potential ISIS recruits, including children, from camps and prisons throughout Syria.[52] Some fundraising networks generated funds for this specific purpose in Indonesia, Türkiye, the United States, and elsewhere, which were then transferred via hawala networks to al-Hawl, an ISIS displacement camp in Syria.[53]

ISIS continues to extensively utilize traditional methods to move and transfer funds, such as hawala and cash, but the group has also adopted widespread use of mobile money service providers, particularly in Eastern and Central Africa.[54] ISIS also utilizes regional financial hubs, such as Türkiye, as conduits for moving and raising money on behalf of the group. Notably, in 2023, ISIS-K used Türkiye as a transit hub for disbursing funds and transferring operatives and weapons from Afghanistan to Europe for possible attacks.[55] In 2023, the United States and Türkiye jointly designated several members of an ISIS financial facilitation network, indicating ISIS's reliance on hawala businesses in Türkiye and Iraq for financial transactions. This network managed several hawala offices and oversaw the transfer of funds from Persian Gulf-based donors to ISIS.[56] In late 2021, the United States designated Ismatullah Khalozai, who was operating "a Türkiye-based hawala business to transfer funds to finance ISIS-K

48 CIFG Fact Sheet 2023.

49 Department of Treasury, OFAC, "Treasury Designates Senior ISIS-Somalia Financier", (Jul. 27, 2023), https://home.treasury.gov/news/press-releases/jy1652.

50 Id., UN Analytical Support and Sanctions Monitoring Team, *Sixteenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat*, (Feb. 1, 2023) (16th Report of UN SG on ISIS), https://undocs.org/S/2023/76.

51 UN Analytical Support and Sanctions Monitoring Team, *31st Report of the Analytical Support and Sanctions Monitoring Team*, p.18, (Feb. 13, 2023) (31st UN MT Report), N2303891.pdf (securitycouncilreport.org).

52 Department of Treasury, OFAC, "Treasury Designates Facilitation Network Supporting ISIS Members in Syria", (May 9, 2022), https://home.treasury.gov/news/press-releases/jy0772.

53 Id.

54 UN MT 31st Report, p. 18.

55 CIFG Fact Sheet 2023.

56 Department of Treasury, OFAC, "The United States and Türkiye Take Joint Action to Disrupt ISIS Financing", (Jan. 5, 2023), https://home.treasury.gov/news/press-releases/jy1181.

operations."[57] Before that, Khalozai was involved in another financing scheme out of the United Arab Emirates (UAE) and was engaged in human smuggling operations in Afghanistan, both of which benefitted ISIS-K.

ISIS-related activity in the United States. is largely relegated to lone, self-radicalized individuals seeking to conduct ISIS-inspired attacks, travel abroad to join ISIS, or offer financial support to the group. Financial activity linked to ISIS in the United States typically involves supporters collecting or sending small amounts of money abroad or financing their own or others' travel to ISIS conflict zones. This money generally comes from legal means, often personal savings, and sometimes may be collected on behalf of others. Individuals may coordinate the donations through encrypted mobile applications like Telegram, send the funds in the form of virtual assets, wire them abroad through a fiat money service business (MSB), or, if collected in cash, pass them to couriers. Some U.S. persons have also engaged in more extensive financial and fundraising activity on behalf of ISIS.

- In May 2023, U.S. authorities arrested an American citizen and charged him with attempting to provide material support to a designated foreign terrorist organization, in the form of collecting, transmitting, receiving, and distributing money to ISIS members.
- In November 2022, a Connecticut man pleaded guilty to attempting to provide material support to ISIS.[58] According to court records, beginning in approximately September 2018, Ahmad Khalil Elshazly, a U.S. citizen, expressed a desire to travel to Syria and the surrounding area to fight on behalf of ISIS. In December 2019, Elshazly paid $500 to a person he believed was an ISIS facilitator who would be able to smuggle him out of the U.S. to Turkey.[59]
- In October 2023, an American citizen was indicted for knowingly concealing the source of material support or resources that he intended to go to ISIS. According to the charging documents, the defendant provided multiple gift cards to an individual he believed was an ISIS supporter with the intention that the gift cards be sold on the dark web for a little less than face value and resulting profits be used to support ISIS. The defendant allegedly stated that he wanted the proceeds to go to ISIS "for war on kuffar," (disbelievers). In total, it is alleged that between January and May 2023, he donated $705 intended to support ISIS.

Al-Qa'ida (AQ)

Like ISIS, AQ has continued to suffer losses in senior leadership over the past two years, which has further advanced the decentralization of the group.[60] However, AQ's presence across the African continent through local affiliates like al-Shabaab and al-Qa'ida in the Islamic Maghreb (AQIM) still represents a potent threat to regional and global security. These affiliates continue to exploit security gaps and weak state institutions, especially in Somalia, to consolidate power and retain control. IC assessments note that AQ maintains its ideological commitment to attacking Western interests and targets, and this threat is heightened in regions where AQ maintains territorial control, such as in Somalia, the Sahel, and parts

57 Department of Treasury, OFAC, "Treasury Designates Key Financial Facilitator for the Islamic State's Afghanistan Branch", (Nov. 22, 2021), https://home.treasury.gov/news/press-releases/jy0502.

58 Department of Justice, "Connecticut Man Admits to Attempting to Travel to The Middle East to Join and Fight For ISIS", (Nov. 30, 2022), https://www.justice.gov/opa/pr/connecticut-man-admits-attempting-travel-middle-east-join-and-fight-isis.

59 Id.

60 Department of State, "The Death of Ayman al-Zawahiri", (Aug. 1, 2022), The Death of Ayman al-Zawahiri - United States Department of State.

of Western Africa.[61] AQ also has collaborated with the Taliban in Afghanistan, and U.S. and UN officials have confirmed that AQ's new leader, Saif al Adel, is currently residing in Iran.[62]

AQ and affiliate groups continue to utilize many of their long-standing methods of illicit revenue generation. According to the UN, al-Shabaab is still in a very strong financial position, having several reliable sources of income, with an estimated annual revenue of around $100 million.[63] The group engages in systemic extortion of businesses and individuals in Somalia, leveraging its territorial control to maintain a consistent stream of revenue.[64] Tactics include setting up checkpoints to extort vehicles and transportation of goods along supply routes as well as illegally taxing residential properties and developers of new properties in Mogadishu.[65] Al-Shabaab predominantly collects this money in cash but also uses mobile money services, money remitters, and banks to transfer funds.[66] Recent public actions against al-Shabaab financiers have highlighted al-Shabaab's reliance on weak government institutions and regional and international networks of financial facilitators to support the group's activities.

In October 2022, Treasury designated a network of al-Shabaab financial facilitators in Somalia who materially assisted the group and provided an array of services, from weapons procurement to recruitment.[67] This network played a key role in a smuggling and weapons trafficking network in Yemen that was utilized by al-Shabaab as well as other criminal enterprises.[68] One designated individual, Ahmed Hasan Ali Sulaiman Mataan, was a Somali businessman who operated a fleet of ships used to traffic weapons and improvised explosive device components from Yemen on behalf of al-Shabaab. Other members of the network acted as intermediaries for Al-Shabaab, operating between the group and businesses and NPOs in Somalia through facilitating funds transfers, collecting money, and fundraising for Al-Shabaab.[69] Another individual, Hassan Afgooye, is a key leader within al-Shabaab and has helped with numerous illicit financial activities on behalf of the group, including operating sham charities, fundraising, racketeering, and kidnapping.

A subsequent Treasury action in May 2023 highlighted another financial network of al-Shabaab facilitators, including an extensive charcoal smuggling network that provided income to the group.[70] Members of the illegal charcoal smuggling operation acted in contravention of a 2012 UN Security Council Resolution banning the import of Somali charcoal due to its role in funding various criminal

61 ODNI 2023 Annual Threat Assessment, p. 32.

62 Department of State, Department Press Briefing, (Feb. 15, 2023), https://www.state.gov/briefings/department-press-briefing-february-15-2023/#post-420718-Iran4.

63 Department of Treasury, OFAC, "Treasury Designates al-Shabaab Financial Facilitators", (Oct. 17, 2022), https://home.treasury.gov/news/press-releases/jy1028.

64 Hiraal Institute, *A Losing Game: Countering Al-Shabab's Financial System*, (Oct. 2020), (A Losing Game), https://hiraalinstitute.org/wp-content/uploads/2020/10/A-Losing-Game.pdf.

65 Africa Center for Strategic Studies, "Reclaiming Al Shabaab's Revenue", (Mar. 27, 2023), https://africacenter.org/spotlight/reclaiming-al-shabaabs-revenue/; A Losing Game, p. 4.

66 UN Sanctions Committee, *Final Report of the Panel of Experts on Somalia*, p. 15, (Oct. 2, 2023), 231024401.pdf,

67 Department of Treasury, OFAC, "Treasury Designates al-Shabaab Financial Facilitators", (Oct. 17, 2022), https://home.treasury.gov/news/press-releases/jy1028.

68 Id.

69 Id.

70 Department of Treasury, OFAC, "Treasury Designates Terror Operatives and Illicit Charcoal Smugglers in Somalia", (May 24, 2023), https://home.treasury.gov/news/press-releases/jy1499.

and terrorist groups and contributing to conflict and instability within Somalia. The charcoal smuggling network helped coordinate the sale and shipment of charcoal from Somalia to Persian Gulf countries, such as Oman and the UAE. The main interlocutor, Ali Ahmed Naaji, operated a legitimate Somalia-based international business that also funded al-Shabaab. Other members of the network assisted with fraudulent paperwork, disguising the charcoal cargo for shipment, and utilizing their own registered businesses to broker the deals.

Financial activity linked to AQ in the United States generally consists of U.S. citizens providing or attempting to provide financial support to AQ or AQ-linked groups using personal funds transferred abroad, sometimes utilizing registered MSBs.

- In July 2022, a U.S. citizen, Georgianna A.M. Giampietro, was sentenced to 66 months in prison for concealing material support and resources intended to be provided to the U.S.- and UN-designated Hayat Tahrir al-Sham (HTS), an AQ-linked terrorist group in Syria.[71] According to court documents, in September 2018, Giampietro had conversations with an undercover agent who expressed interest in traveling to Syria to join HTS. The undercover agent told Giampietro that her husband swore an oath of allegiance to HTS and that he intended to fight on behalf of HTS. Giampietro initially provided instruction and advice to the undercover agent on how to travel to Syria in order to avoid detection by law enforcement. In subsequent conversations with the undercover agent, Giampietro offered to communicate with her contacts on their behalf to assist them in safely traveling to Syria to join HTS and later provided the undercover agent with her contact's information to assist her and her husband in their travel to Syria. In addition, Giampietro intended that the undercover agent and her husband would provide funds to that person, who would in turn provide funds to HTS, thereby providing material support to HTS disguised as a charitable contribution. Giampietro sent money to a charitable organization that purported to help widows and orphans in Syria but actually supported militant jihad in Syria and aided HTS.[72]
- In January 2023, a U.S. citizen, Maria Bell, was sentenced to 34 months in prison for concealing attempts to provide material support to al-Nusrah Front (ANF) and HTS.[73] According to documents filed in court, beginning at least as early as March of 2017, Bell used mobile applications to communicate with and provide advice to fighters based in Syria who were members of various factions fighting the Assad regime. The charges against Bell centered on her communication with, and provision of money to, one specific fighter based in Syria, who was a self-identified member of HTS. Notably, Bell sent cryptocurrency to this fighter via an MSB using an intermediary to conceal the source of the funds, and also provided him with advice on weapons and ammunition.

71 Department of Justice, "Sparta Woman Sentenced to 5 ½ Years in Prison for Concealing Material Support Intended for a Foreign Terrorist Organization", (Jul. 20, 2022), https://www.justice.gov/usao-mdtn/pr/sparta-woman-sentenced-5-12-years-prison-concealing-material-support-intended-foreign.

72 USA v. Giampietro, Case 2:19-cr-00013 (Sentencing Memorandum Opinion and Order), (D. MD Tenn. Jul. 11, 2022) p. 11-12.

73 Department of Justice, "Sussex County Woman Sentenced to 34 Months in Prison for Concealing Terrorist Financing to Syrian Foreign Terrorist Organizations", (Jan. 24, 2023), https://www.justice.gov/usao-nj/pr/sussex-county-woman-sentenced-34-months-prison-concealing-terrorist-financing-syrian.

Hizballah

Hizballah has maintained its ideological commitment to diminishing the U.S. presence in the Middle East. Through its sophisticated global financing network and advanced conventional military capabilities, it maintains the capability to threaten U.S. interests at home and abroad.[74] Hizballah leverages a worldwide network of illicit businesses, criminal enterprises, and financial facilitators to maintain a robust global presence and raise and launder large amounts of money.

Hizballah is funded in large part by the Iranian government, which provides several hundred million dollars a year in direct funding.[75] Hizballah also engages in a range of illicit and commercial activities to supplement its income. These illicit activities range from oil smuggling and shipping and charcoal smuggling to drug and weapons trafficking. For instance, Hizballah has been implicated in several complex illicit oil smuggling schemes which were orchestrated by, and jointly benefitted, both Hizballah and Iran's Islamic Revolutionary Guard Corps (IRGC) Qods Force.[76] In one scheme, numerous companies and ships smuggled Iranian oil by blending it with Indian petroleum-products and creating counterfeit certificates of origin. The oil was then loaded onto ships owned by a front company and flagged in Liberia and Djibouti, seen as more permissive jurisdictions, to avoid scrutiny. This example demonstrates Hizballah's ability to use a complex web of front companies to obfuscate both the ownership of the vessels and the true source of the oil.

Hizballah also regularly exploits the international financial system and excels in utilizing networks of seemingly legitimate front companies to raise, launder, and move money on behalf of the group.[77] These front companies are used to obscure the true beneficial ownership. They are used extensively in various commercial activities benefiting Hizballah, such as real estate, import/export, construction, and luxury goods.[78] These commercial activities generate significant income for the group and draw less scrutiny than outright illicit enterprises.

Hizballah relies on jurisdictions with weak government institutions, porous borders, or corrupt state officials to facilitate their illicit activities. Historically, such areas have included parts of South America, particularly the tri-border area of Brazil, Paraguay, and Argentina, as well as some parts of West Africa and the Middle East, where key financial facilitators assist in transferring and moving funds on behalf of the group.[79] In one example, two Hizballah supporters and prominent businesspeople in Guinea assisted in moving funds from Guinea to Hizballah, and utilized political connections, bribes, and access to corrupt officials to send cash in U.S. dollars in suitcases out of Conakry airport.[80] Hizballah also draws on individual financial contributions from sympathetic members of the Lebanese diaspora located around the world in many of the jurisdictions mentioned above.

74 ODNI 2023 Annual Threat Assessment pp. 31-33.

75 International Centre for Counter-Terrorism, *An interview with Matthew Levitt on the role of Hezbollah in Israel*, (Oct. 27, 2023), https://www.icct.nl/publication/interview-matthew-levitt-role-hezbollah-israel.

76 Department of Treasury, OFAC, "Treasury Sanctions Oil Shipping Network Supporting IRGC-QF and Hizballah", (Nov. 3, 2022), https://home.treasury.gov/news/press-releases/jy1076.

77 Department of Treasury, OFAC, "Treasury Targets Hizballah Financial Network's Abuse of the Business Sector", (May 19, 2022), https://home.treasury.gov/news/press-releases/jy0796.

78 Department of Treasury, OFAC, "Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hizballah Financier", (Apr. 18, 2023), https://home.treasury.gov/news/press-releases/jy1422.

79 Department of Treasury, "Treasury Sanctions Hizballah Financiers in Guinea", (Mar. 4, 2022), https://home.treasury.gov/news/press-releases/jy0631.

80 Id.

As noted in prior NTFRAs, Hizballah still maintains a footprint within the United States. Hizballah members and sympathizers have long been involved in an array of large-scale criminal schemes, including sophisticated money laundering, smuggling, and trafficking networks that have involved the U.S. financial system.[81] In the past, Hizballah and its supporters have regularly transferred funds through the U.S. financial system. However, some case examples have highlighted Hizballah activity within the United States that is focused more on information-gathering or, in very isolated cases, potential preparation for attacks rather than generating revenue. As noted below, there are also instances of Hizballah operatives attempting to purchase military or export-controlled equipment, including through the use of front companies.

- In April 2023, Treasury and Justice disrupted a large international money laundering and sanctions evasion network involving over 52 people and entities located across the globe.[82] These individuals and entities were involved in an array of activities including the transfer, shipment, and delivery of cash, precious gems, art, and luxury goods on behalf of Hizballah. This network stretched across Africa, Western Europe, the Middle East, and Asia and utilized hubs in the UAE, South Africa, Lebanon, and Hong Kong. According to court documents, Nazem Said Ahmad, who was sanctioned by the United States in 2019 for being a financier for Hizballah, and his co-conspirators, including family members and business associates, relied on a complex web of business entities to obtain valuable artwork from U.S. artists and art galleries and to secure U.S.-based diamond-grading services all while hiding Ahmad's involvement in and benefit from these activities.[83] Over one hundred million dollars in transactions involving artwork and diamond-grading services flowed through the U.S. financial system.
- In May 2023, Alexei Saab was sentenced to 12 years in prison for receiving military-type training from a designated foreign terrorist organization (Hizballah), marriage fraud, conspiracy, and making false statements.[84] According to court documents, Saab joined Hizballah in 1996 and transitioned to Hizballah's external operations unit, the Islamic Jihad Organization (IJO), where he received extensive training in IJO tradecraft, weapons, and military tactics. In 2000, Saab entered the United States and remained an IJO operative, continuing to receive military training in Lebanon and conducting numerous operations for the IJO. This included intelligence collection against potential attack targets, as well as opening a front company that he could use to obtain fertilizer in the United States for use as an explosives precursor. Finally, in or about 2012, Saab entered into a fraudulent marriage in exchange for $20,000. The purpose of the marriage was for Saab's purported wife to apply for her citizenship.
- A review of financial institution reporting from 2021-2022 highlighted that individuals linked to known and previously designated Hizballah financiers routinely used the U.S. financial system to transfer funds through a range of financial institutions located in the United States and abroad.[85]

81 See 2022 NTFRA pp. 11-12.

82 Department of Treasury, OFAC, "Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hizballah Financier", (Apr. 18, 2023), https://home.treasury.gov/news/press-releases/jy1422.

83 Department of Justice, "OFAC-Designated Hezbollah Financier and Eight Associates Charged with Multiple Crimes Arising Out of Scheme to Evade Terrorism-Related Sanctions", (Apr. 18, 2023), https://www.justice.gov/opa/pr/ofac-designated-hezbollah-financier-and-eight-associates-charged-multiple-crimes-arising-out.

84 Department of Justice, "New Jersey Man Sentenced To 12 Years in Prison for Receiving Military-Type Training From Hezbollah, Marriage Fraud and Making False Statements", (May 23, 2023), https://www.justice.gov/opa/pr/new-jersey-man-sentenced-12-years-prison-receiving-military-type-training-hezbollah-marriage.

85 Treasury analysis of financial institution reporting.

Hamas

Harakat al-Muqawama al-Islamiya (Islamic Resistance Movement), better known by the acronym Hamas, is a U.S.-designated terrorist group primarily based in the Gaza Strip and the West Bank since its formation as an offshoot of the Muslim Brotherhood in the late 1980s. Hamas is committed to waging violent jihad against Israel and liberating Palestine through violent resistance. Hamas has been designated as a terrorist group by the United States since 1997.[86] Since 2005, Hamas has been the governing authority in the Gaza Strip and has maintained a presence in the West Bank, intermittently provoking regional instability in the 1990s and throughout the 2000s by committing terrorist attacks and violence directed at Israel. The October 7, 2023, terrorist attacks, which Hamas perpetrated on Israel and the citizens of at least 36 other nations, underscored Hamas's commitment to its extremist goals and brought renewed global attention to the financing and operations of the group.

Hamas has advanced military capabilities at its disposal, partly as a result of decades of accumulating weapons through Iranian government support, as well as forming extensive and complex global financing networks. Hamas is unique among other terrorist groups because its cause is viewed sympathetically by some governments and the general public in some countries with Muslim-majority populations. Notably, Hamas is not designated as a terrorist organization in most of the Middle East, and this permissive regional environment has allowed Hamas facilitators or operatives to freely raise and transfer funds.

Hamas is a well-resourced group that garners substantial financial resources from numerous and diverse sources.[87] Due to its territorial control of the Gaza Strip, Hamas historically has been able to exploit its position as a governing entity to generate considerable revenue, in part by extorting the local population. The group's primary external funding comes from Iran, which has provided it roughly $100 million per year. Hamas also generates of revenue from an expansive and sophisticated international investment portfolio, previously estimated to be worth at least $500 million.[88] This investment portfolio has invested in companies and assets located across the world, including in Algeria, Saudi Arabia, Sudan, Türkiye, and the UAE, and is managed by Hamas' Investment Office.[89] In addition, Hamas relies on a global fundraising network to raise funds for its nefarious activities. Hamas is prolific in soliciting donations from witting and unwitting donors worldwide in both fiat and virtual assets.

Hamas facilitators have used numerous methods to collect and transfer funds into the Gaza Strip. These include crowdfunding websites and sham charities, where in some cases, the destination of the funds was concealed under the guise of humanitarian efforts. In other cases, they solicited funds directly for their cause from sympathetic donors. Hamas has also used complicit VASPs and money transmitters throughout the globe to move funds. In the aftermath of the October 7, 2023, terrorist

86 The European Union, members of the G7, as well as some other countries have fully designated the entirety of Hamas as a terrorist organization.

87 Following Hamas' terrorist attack, Treasury issued an alert to U.S. financial institutions highlighting Hama's main sources of funding and identifying red flag indicators relating to Hamas' terrorist financing activity. These indicators include transactions that originate with or involve entities that have a nexus to Iran-supported terrorist groups such as Hizballah or Palestinian Islamic Jihad (PIJ); charitable organizations soliciting donations without appearing to provide any charitable services, and transactions involving MSBs or financial institutions in higher-risk jurisdictions that are tied to Hamas activity and that are reasonably believed to have lax Customer Due Diligence (CDD) or AML/CFT practices, see FinCEN Alert, FIN-2023-Alert006, October 20, 2023.

88 Department of Treasury, OFAC, "Treasury Targets Covert Hamas Investment Network and Finance Official", (May 24, 2022), https://home.treasury.gov/news/press-releases/jy0798.

89 Id.

attacks, Treasury designated a Gaza-based VASP called Buy Cash Money and Money Transfer Company for serving as a key node in Hamas's virtual asset fundraising schemes.[90] The same entity has also been identified as being involved with funds transfers on behalf of other terrorist groups.[91]

Hamas's global financial footprint and use of the regulated international financial system means that its facilitators likely have access to the U.S. financial system, particularly as Hamas has sought to raise funds from international supporters. U.S. persons have been convicted of providing or conspiring to provide material support to Hamas from the United States in recent years.[92] After the October 2023 terrorist attacks, Hamas supporters around the world mobilized global fundraising efforts on behalf of the group. These online fundraisers took various forms, often seeking to collect money on crowdfunding sites under the guise of charitable donations for Gaza.

VULNERABILITIES

Registered Money Services Businesses (MSBs)

As noted in past NTFRAs, registered MSBs, including money transmitters,[93] play an integral role in the non-bank financial institution ecosystem, providing necessary financial services to unbanked and underbanked populations and facilitating billions of dollars in funds transfers for legitimate purposes around the world. However, MSBs have been, and continue to be, vulnerable to terrorist financing for several reasons. Their global reach, their role as the sole financial services provider in some jurisdictions, along with weaknesses in the implementation and supervision for AML/CFT requirements in some foreign jurisdictions, and their less stringent requirements than other financial institutions such as banks make them an attractive option for terrorist financing.

Numerous terrorist groups have been identified as using money transmitters to move funds. Hizballah has routinely used money remitters to move funds around the world. For example, in January 2023, Treasury identified a Lebanese MSB called CTEX that was owned by Lebanon-based economist Hassan Moukalled, who provided financial advisory services to Hizballah.[94] CTEX was established as a front company in 2021 and by 2022 was transmitting millions of dollars in U.S. currency, including "providing U.S. dollars to Hizballah institutions."[95] Additionally, a review of financial institution reporting identified individuals connected to Hizballah who used MSBs to transfer funds globally.

In the United States, MSBs are subject to AML/CFT regulations imposing AML program, reporting, and recordkeeping obligations. A range of activities qualify a business as being an MSB, such as currency

90 Department of Treasury, OFAC, "Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators", (Oct. 18, 2023), https://home.treasury.gov/news/press-releases/jy1816.

91 Id.

92 See, for example, Department of Justice, "Somerset County Man Admits Concealing Material Support to Hamas", (Sep. 15, 2020), https://www.justice.gov/opa/pr/somerset-county-man-admits-concealing-material-support-hamas, and Department of Justice, "Second Member Of "Boogaloo Bois" Pleads Guilty to Conspiracy to Provide Material Support to Hamas", (May 4, 2021), https://www.justice.gov/opa/pr/second-member-boogaloo-bois-pleads-guilty-conspiracy-provide-material-support-hamas.

93 While VASPs may also be registered as MSBs, their vulnerability is being addressed holistically in the VASPs section below.

94 Department of Treasury, OFAC, "Treasury Sanctions Key Hizballah Money Exchanger", (Jan. 24, 2023), https://home.treasury.gov/news/press-releases/jy1211.

95 Id.

exchange; check cashing; money transmission, including through VASPs; providing or selling prepaid access; and any business issuing or cashing travelers checks or money orders.[96] MSBs have a lower SAR filing threshold ($2,000) than other regulated financial institutions ($5,000).[97] MSBs are required to file suspicious activity reports (SARs), and an analysis of SAR reporting shows that between 2020 and 2022, MSBs filed nearly 72% of all SARs related to TF.[98]

Large MSBs have a significant global footprint that can go beyond the reach of most traditional banking institutions. Such entities generally have advanced internal controls and compliance programs in accordance with the risk of the jurisdictions in which they do business, which tend to be higher risk than where banks operate. However, smaller MSBs, such as those that may only undertake small-scale transactions or perform only one of the services that may qualify them as an MSB (*e.g.*, a grocery store that also provides services as a dealer in foreign exchange), may face higher TF risks. These small MSBs may have weaker AML/CFT programs and less oversight than established global MSB businesses, or they may devote fewer resources to monitoring suspicious activities than their larger counterparts. There are also several instances where money remitters outside of the United States have been owned by or employed terrorist supporters who have knowingly facilitated financial activity on behalf of these groups.

Person-to-Person (P2P) Payments

Depending on the platform, a person-to-person (P2P) payment can be initiated from a consumer's online bank account or prepaid card account through a mobile or desktop application (apps). P2P apps are free to download, and payments are typically free when made using a linked checking account, debit card, or stored balance; some platforms also allow funding via credit card for a fee. P2P services operate as relatively closed environments where users can only send funds to another individual on the same platform. Because of this feature, bank account details can be kept private from other users: all that is typically required from users to send a payment is the recipient's email address or phone number. When users receive a payment, they usually have the option of maintaining a balance in the app or transferring the funds to their bank accounts. While most P2P services in the United States only operate domestically, some offer cross-border payment options. As money transmitters, P2P payment services are considered MSBs and thus subject to the reporting, recordkeeping, and AML/CFT program requirements under the Bank Secrecy Act (BSA) and must register with FinCEN.

P2P payment platforms have brought accessibility, ease, and inclusion to the regulated financial system for many individuals worldwide. These services have become particularly important for unbanked and underbanked individuals who may reside in extremely rural areas and do not otherwise have access to regulated banking services. These payment methods are not necessarily inherently more risky than traditional banking systems, but the speed and ease with which individuals can perform these transactions can make them an attractive option for criminals or terrorists. Additionally, incorporating P2P payment systems in conjunction with more traditional forms of moving and storing money, such as cash and hawala, can make a money trail significantly more complex.

96 See Money Services Business Definition | FinCEN.gov.

97 See 31 C.F.R. 1022.210(d)(1)(i)(A).

98 SAR Stats | FinCEN.gov.

Unregistered Money Transmission

People may choose to use unregistered money transmitters in areas without access to the regulated financial system. However, unlike registered MSBs, these money transmitters operate without complying with the core AML/CFT program or the recordkeeping and reporting requirements that apply to registered MSBs, increasing the risk of exposure to illicit activity. A variety of bad actors may seek out or operate as unregistered money transmitters to facilitate illicit conduct, as people may perceive these businesses as less transparent – and their transactions thus more difficult to trace. For example, unregistered money remitters remain a vulnerability through which groups such as AQ and ISIS move money internationally, especially because the lack of registration in the United States prevents law enforcement from being apprised of suspicious money transmission activity.

While unregistered money transmitters have offered more traditional financial services (where funds are transferred through an account the unregistered remitter maintains at a financial institution), a growing number of online payment providers or social media companies are, in some cases, acting as unregistered money transmitters. In addition, individuals and entities operating as VASPs in the United States but not registered with FinCEN are acting as unregistered money transmitters. As a recent enforcement case demonstrates (discussed in more detail below), unregistered money transmitters may have significant ties to terrorist financing.[99]

Cash

Cash, and in particular, U.S. dollars, continues to be a fixture for terrorists raising, moving, and using funds, particularly when transferring funds across borders. While using cash is slower, bulkier, and less efficient than other mechanisms of moving funds, the anonymity, liquidity, and lack of electronic footprint mean that a cash-based money trail is more difficult to track and avoids the scrutiny that comes with transactions executed through a regulated financial institution.

As detailed in the 2022 NTFRA, U.S.-based supporters of ISIS still use cash to fund foreign travel or otherwise support the group. DVE groups or others inspired to conduct attacks in the United States also use cash to purchase weapons or materials to make explosives.

- In June 2022, a U.S. resident, Dilkayot Kasimov, was sentenced to 15 years in prison for conspiring and attempting to provide material support to ISIS in the form of cash.[100] According to court documents, in 2015, Kasimov's co-conspirators planned to travel to Syria to fight on behalf of ISIS. Kasimov provided money – his own and cash collected by others – to help fund a co-conspirator's travel and expenses. In February 2015, Kasimov traveled to John F. Kennedy International Airport and handed $1,600 in cash on behalf of himself, a co-conspirator, and others to a would-be foreign fighter.
- Two U.S. citizens were sentenced in February 2023 for attempting to provide material support to ISIS.[101] According to court documents, the couple were ISIS supporters who sought to travel to the Middle East to join and fight for ISIS. One of the defendants provided $1,000 in cash as travel costs to an undercover law enforcement officer.[102]

99 See U.S. Department of Treasury, "U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws", (Nov. 21, 2023), https://home.treasury.gov/news/press-releases/jy1925.

100 Department of Justice, "Funder of ISIS Foreign Fighter Sentenced to 15 Years in Prison", (Jun. 3, 2022), https://www.justice.gov/opa/pr/funder-isis-foreign-fighter-sentenced-15-years-prison.

101 Department of Justice, "New York Man and Alabama Woman Sentenced for Attempting to Provide Material Support to ISIS", (Feb. 3, 2023), https://www.justice.gov/opa/pr/new-york-man-and-alabama-woman-sentenced-attempting-provide-material-support-isis.

102 Id.

Banks

Banks are key participants in the global financial system. U.S. banks specifically facilitate the majority of transactions that are processed on a day-to-day basis through the global financial system. Among the services that banks provide are correspondent banking services that enable foreign respondent banks to conduct business and provide services to customers in foreign markets through correspondent banks that hold accounts at U.S. financial institutions. The ability to make and receive international payments through correspondent banking relationships is vital for facilitating trade and commerce, thus promoting sustained economic growth worldwide. Most large U.S. and European banks have appropriate AML/CFT programs that comply with the BSA and other AML/CFT regulatory requirements, and also maintain sophisticated risk mitigation and monitoring practices. The sheer volume of transactions flowing through the global banking system makes it particularly challenging for banks to identify terrorist-related transactions, meaning the inherent risk of U.S. and global banks' exposure to illicit activity is high.

Because of the structure of the activity and the limited information regarding the nature or the purpose of underlying transactions, correspondent banks face increased exposure to TF risks. Moreover, respondent banks may be located in higher-risk jurisdictions where the AML/CFT regime is weaker, and the correspondent bank cannot confidently rely on the due diligence and compliance measures of the respondent bank. For example, geographic shifts of terrorism financing centers over the past several years away from the Middle East and towards Africa have put more pressure on the financial institutions that operate in and with jurisdictions with weak governance and AML/CFT regimes, making correspondent banking vulnerabilities more acute.

In some countries, terrorists have seized control of existing regime structures, restricting access by state institutions to the international financial system. These restrictions have prevented illicit actors from transacting funds through the global banking system. Terrorist control of state regime structures may have long-term implications for achieving important public interest objectives such as addressing poverty and promoting overall financial inclusion, facilitating the delivery of humanitarian aid, and promoting sustained economic growth and development.

NPOs, charities, MSBs, and other non-bank entities play key roles in implementing these policy objectives—the success of which relies on sustained access to financial services. Bank decisions to establish and maintain such relationships are generally based on evaluations of ML/TF and other illicit finance risks associated with these customers, and the jurisdictions where they operate, along with profitability. Where the ML/TF risks are outside its risk tolerance, or the institution does not have the risk mitigation resources to effectively address the TF or other illicit finance risks, including experience with the customers' business activities and monitoring transactions to detect suspicious activity, financial institutions may disengage with certain banking relationships (*i.e.*, de-risking).[103] If NPOs or MSBs lose access to the formal financial system, these entities may resort to using alternative mechanisms outside the regulated financial system, and this loss of transparency affects governments ability to monitor transactions and can increase their exposure to TF activity.[104]

Additionally, groups like Hamas or Hizballah that are not consistently designated as terrorist

103 Department of Treasury, *The Department of the Treasury's De-risking Strategy,* (Treasury De-risking Strategy), p.16, (Apr. 2023), https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf.

104 Treasury De-risking Strategy, p. 36.

organizations globally are able to exploit gaps in sanctions designations to raise and move funds using the international financial system. Though the United States has domestically designated these groups, they have not been designated by the United Nations Security Council and therefore UN member states are not obligated to domestically impose these sanctions. These global sanctions designation gaps allow individuals associated with these terrorist groups to open bank accounts and transact freely in some regions, thereby increasing the potential terrorist financing exposure of U.S. correspondent banks.

Virtual Assets

This report uses the terms virtual asset and VASP, terms not contained explicitly in U.S. law or regulation, to align with the terminology defined by the FATF.[105] Virtual assets, as used in this report, include non-sovereign-administered digital assets (such as convertible virtual currencies (CVCs), like bitcoin and stablecoins)[106] but do not cover central bank digital currencies (CBDCs), which are representations of fiat currency and treated the same as fiat currency by the FATF or representations of other financial assets, such as digitized representations of existing securities or deposits.[107] 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.

In the United States, VASPs have AML/CFT obligations if they fall under the BSA's definition of a financial institution, which covers banks, broker-dealers, mutual funds, MSBs, futures commission merchants (FCMs), and introducing brokers, among others.[108] Many VASPs in the United States are considered MSBs, and some may be mobile payment platforms. VASPs that operate wholly or in substantial part in the United States are considered MSBs, unless an applicable exemption applies, and must comply with applicable BSA requirements. Depending on the VASP's activities, they may also be considered FCMs or broker dealers. Each of these financial institutions has AML/CFT

105 Financial Action Task Force, "FATF's Focus on Virtual Assets", https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets. html?hf=10&b=0&s=desc (fatf_releasedate).

106 Stablecoins are digital assets that are designed to maintain a stable value "pegged" to a national currency or other reference assets. As with all digital assets, stablecoins can present ML/TF risks. The magnitude of these risks depends on various factors, including the application of AML/CFT controls, the degree to which it is adopted by the public, and the design of the stablecoin arrangement. For additional information, see the President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency's Report on Stablecoins (November 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

107 CBDCs may have unique ML/TF risks compared with physical fiat currency, depending on their design, and such risks should be addressed prior to launch. CBDCs may also present opportunities to program AML/CFT controls into the CBDCs or related service providers, but these opportunities should also take into consideration data privacy and other concerns.

108 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

obligations, including requirements to establish and implement an AML program[109] and recordkeeping and reporting requirements, including SAR requirements.[110] Additionally, all VASPs subject to U.S. jurisdictions have sanctions compliance obligations.

The U.S. government assesses that both international terrorist and DVE groups have continued using virtual assets to generate and transfer funds. Since the 2022 NTFRA, certain terrorist groups, such as ISIS-K and Hamas, have increased their understanding of and are experimenting with different types of virtual assets. However, the U.S. government assesses that terrorists still prefer traditional financial products and services. This preference is likely in part due to the price volatility of many virtual assets, the limited ability to purchase goods and services with virtual assets, and a lack of infrastructure necessary to exchange virtual assets for fiat currency in some jurisdictions where terrorist groups operate.

In contrast to the 2022 NTFRA, which identified that terrorist groups most frequently solicited virtual asset donations of bitcoin, terrorist groups soliciting donations of virtual assets are increasingly turning to stablecoins, which are virtual assets that are designed to maintain a stable value relative to a national currency or other reference assets. Stablecoins purport to be less volatile than other virtual assets and may enable terrorist groups to utilize virtual assets while mitigating the financial risks associated with price fluctuations. Additionally, stablecoins may be preferred by VASPs used by terrorists to exchange virtual assets for fiat currency. Reporting and private sector analysis indicate that ISIS and other terrorist groups have moved towards using stablecoins, including Tether, to move or store funds.[111,112]

Consistent with the 2022 NTFRA, most cases of terrorists using virtual assets involve groups fundraising online and specifically soliciting virtual assets from donors. Such fundraising campaigns are often disseminated through social media or encrypted apps like Telegram and often solicit funds in virtual assets and fiat currency, enabling the donor to decide which method to use. Individual donors can send virtual assets from a VASP or an unhosted virtual asset wallet[113] to a virtual asset address owned by the terrorist group. Groups may use the funds for a range 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 virtual assets for fiat currency.[114]

109 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). An AML Program must include, at a minimum, (a) policies, procedures, and internal controls reasonably designed to achieve compliance with the provisions of the BSA and its implementing regulations; (b) independent testing for compliance; (c) designation of an individual or individuals responsible for implementing and monitoring the operations and internal controls; and (d) ongoing training for appropriate persons. Rules for some financial institutions refer to additional elements of an AML Program, such as appropriate risk-based procedures for conducting ongoing customer due diligence.

110 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.

111 31st UN MT Report, p.18.

112 See e.g., https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure, How Hamas has utilized crypto, and what may be coming (elliptic.co), Israel Seizes Crypto Wallets Worth $94 Million Linked to Palestinian Islamic Jihad (elliptic.co).

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

114 FATF Crowdfunding for TF Report, pp. 29-30.

Terrorist groups may also use virtual assets to transfer funds to other members or related groups using VASPs or peer-to-peer virtual asset transfers, referring to payments between two unhosted wallets that do not involve a regulated financial institution.[115] In some instances, transfers may take several steps and involve peer-to-peer virtual asset transfers as well as VASPs, including over-the-counter brokers, peer-to-peer virtual asset platforms,[116] or purportedly decentralized exchanges[117], possibly for the purpose of obfuscation. While some of the VASPs used by terrorist groups may be local to their operations, in particular for exchanging virtual assets for fiat currency, they can also leverage VASPs based all over the world to send and receive virtual assets. [118] Regardless of whether terrorist groups received funds from donations or transfers from other groups, they will likely require VASPs to exchange virtual assets for fiat currency, which is often necessary to purchase goods and services.

- In December 2022, DOJ unsealed a criminal complaint charging four defendants with conspiring to provide material support to ISIS. The defendants raised and contributed more than $35,000 through cryptocurrency and other electronic means to bitcoin wallets and accounts they believed to be funding ISIS.

When VASPs operating in the United States or abroad lack or fail to implement AML/CFT requirements, they are vulnerable to misuse for TF. Despite the FATF extending global standards for AML/CFT to VASPs in 2019, many countries have been slow to regulate VASPs. Many VASPs operating abroad have substantially deficient AML/CFT programs, particularly in jurisdictions where international standards for VASPs are not effectively implemented. Based on FATF assessments, jurisdictions are making limited progress (73 out of 98 jurisdictions rated as only partially or not compliant), and a FATF-administered survey found that many jurisdictions had not taken basic steps to assess risk or determine an approach to virtual assets.[119] Uneven and often inadequate regulation and supervision around the world allow VASPs to engage in regulatory arbitrage and expose the U.S. financial system to risk from jurisdictions where regulatory standards and enforcement are less robust.

The FATF has developed a roadmap to encourage countries to implement the FATF standards for virtual assets and VASPs, which includes the planned publication of a table noting progress on implementation for FATF members and jurisdictions assessed to have materially important VASP activities.[120] Although VASPs in the United States have AML/CFT and sanctions obligations, as explained above, there are cases in which VASPs fail to comply with these obligations, raising the risks of exposure to TF and other illicit activity. In some cases, VASPs may not implement AML/CFT controls or other processes to identify customers, enabling misuse by illicit actors, including terrorists. Additionally, VASPs may perceive that they are not subject to U.S. regulatory requirements for AML/CFT

115 For example, ISIS, see CIFG Fact Sheet 2023.

116 P2P service providers, typically natural persons engaged in the business of buying and selling virtual assets rather than safekeeping virtual assets or engaging in P2P transfers on their own behalf, may have regulatory requirements depending on their precise business model.

117 The use of the term "exchange" in this assessment does not indicate registration as such or any legal status of any such platform. This definition is for the purpose of the risk assessment and should not be interpreted as a regulatory definition under the BSA or other relevant regulatory regimes.

118 Department of Treasury, OFAC, "Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators", (Oct. 18, 2023), https://home.treasury.gov/news/press-releases/jy1816.

119 FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, (Jun. 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf.

120 FATF, "Outcomes FATF Plenary, 22-24 February 2023", (Feb. 24, 2023), https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html.

based on their geographic location or the services that they provide.

In November 2023, Binance settled with FinCEN and OFAC for violations of AML and sanctions laws, each assessing the largest civil monetary penalty in their history. Binance did business as a money transmitter in substantial part within the United States, including by cultivating and serving over 1 million U.S. customers through its main platform, but at no time did Binance register with FinCEN. Additionally, Binance failed to file SARs with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and United Nations, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with ISIS, Hamas' Al-Qassam Brigades, Al Qaeda, and the Palestinian Islamic Jihad (PIJ). Although no SARs were filed with FinCEN, Binance has proactively cooperated with global law enforcement and blockchain vendors to combat terrorism financing.[121] While Binance demonstrated its own broad awareness of U.S. sanctions prohibitions, including related to terrorist groups, Binance senior management expressed interest in feigning compliance rather than addressing the company's actual risk.[122] Separately, DOJ charged and secured a guilty plea from both Binance and its founder and chief Executive Officer, Changpeng Zhao, who is currently awaiting sentencing. These settlements were part of a global agreement simultaneous with Binance's resolution of related matters with CTFC and an announcement of DOJ's charges.[123]

Terrorist groups could use anonymity-enhancing technologies such as anonymity-enhanced virtual assets and techniques, like virtual asset mixing, to obfuscate the source, destination, or movement of virtual assets. This technological capability can complicate investigators' ability to trace illicit funds. Based on Treasury's assessments, the use of anonymity-enhancing technologies and techniques for financial transactions by terrorist groups has been limited so far, and Treasury will continue to monitor the use of these services. For example, to increase transparency in the virtual asset ecosystem, FinCEN issued a notice of proposed rulemaking (NPRM) pursuant to section 311 of the USA PATRIOT Act in October 2023 that identifies international convertible virtual currency mixing (CVC mixing) as a class of transactions of primary money laundering concern. FinCEN's proposal would require covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within, or involving jurisdictions outside, the United States. [124]

In contrast, certain elements of virtual assets may support tracing funds associated with terrorist financing. Virtual asset transactions often occur on public blockchains, which means that anyone with internet access can view the pseudonymous transaction data in a public ledger for the blockchain. Public ledgers can support investigations in tracing the movement of illicit funds. However, there are some limitations due to the pseudonymous nature of the data, challenges associated with the use

121 Department of Treasury, FinCEN, *Consent Order Imposing Civil Money Penalty*, (Nov. 21, 2023), https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf.

122 Department of Treasury, OFAC Enforcement Release, "OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Programs", (Nov. 21, 2023), https://ofac.treasury.gov/system/files/2023-11/20231121_binance.pdf.

123 U.S. Department of Treasury, "U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws", (Nov. 21, 2023), https://home.treasury.gov/news/press-releases/jy1925.

124 FinCEN, "FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing", (October 19, 2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

of anonymity-enhancing technologies and techniques, and activity occurring off-chain. Still, recent seizures by Israeli authorities of virtual assets associated with terrorist groups illustrate how public blockchain data can support investigations of terrorist financing in virtual assets and emphasize the critical role that VASPs play in acting on law enforcement information to disrupt terrorist financing. For example, in June 2023, Israeli authorities, with the help of a private sector blockchain analytics firm, seized approximately $1.7 million worth of virtual assets from a VASP allegedly used by Hizballah and Iran's Qods Force to finance their operations, marking the first time such a seizure has been made against Hizballah. Moreover, these disruptions can impact terrorist groups' interest in using virtual assets. In fact, disruptions by U.S. government and Israeli authorities likely contributed to Hamas' announcement in April 2023 that they would no longer receive bitcoin donations after specifically soliciting VA since 2019.[125]

The U.S. government will continue to monitor and assess whether there is more widespread adoption of virtual assets by terrorist groups. For example, as virtual assets become more commonly used across the globe (especially in areas with poor financial and telecommunications infrastructures) and are more widely accepted to pay for goods and services, they may become more popular among terrorist groups.

Non-Profit Organizations (NPOs)

Charitable NPOs play a vital role in delivering humanitarian assistance to vulnerable populations throughout the world. Millions of people residing in crisis or conflict zones rely on the work of charitable NPOs. In the past, certain types of U.S.-based NPOs have been vulnerable to abuse by terrorist groups;[126] however, in the last decade, the charitable sector has made strides in addressing and mitigating the threat posed by TF, including by increasing due diligence measures and risk mitigation efforts, often in collaboration with Treasury and the broader U.S. government.

Today, the vast majority of U.S. charitable NPOs have little exposure to TF.[127,128] Within the United States, only a small subset of charitable NPOs with an international presence are vulnerable to TF. 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.

As noted in the 2022 NTFRA, the U.S. government acknowledges the continued practice of many charitable NPOs to apply internal risk-mitigation measures, including due diligence, governance,

125 Reuters, *Hamas armed wing announces suspension of bitcoin fundraising,* (Apr. 28, 2023), https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/#:~:text=Hamas%20had%20endorsed%20crypto%20as,world%20as%20one%20key%20source.

126 See 2015 National Terrorist Financing Risk Assessment.

127 See 2022 NTFRA, p. 24.

128 This assessment is consistent with the global view that it is a small subset of charitable NPOs that have exposure to terrorist financing. See Best Practices on Combating the Abuse of Non-Profit Organisations (fatf-gafi.org).

transparency, accountability, and other compliance measures, including when responding to crises.[129] Furthermore, implementing partners of the United States Agency for International Development (USAID) active in high-risk environments are also subject to additional vetting measures by USAID. These organizations must implement due diligence and risk-mitigation requirements to ensure full compliance with U.S. sanctions, including threats posed by terrorist organizations.[130]

Despite these measures and Treasury's work to standardize humanitarian-related authorizations across U.S. sanctions programs, some charitable NPOs continue to report challenges accessing financial services or experiencing financial-sector de-risking that interferes with essential, lifesaving services. Certain NPOs may also be targeted with repressive measures that can impact financial access, including misinformation campaigns that may characterize authorized humanitarian activities as diversion. When financial access is lost, some charitable NPOs have reported resorting to payment channels outside the regulated financial sector, which can increase TF risks.[131] Thus, protecting and maintaining access to the banking system is imperative to reduce the TF risk of charitable NPOs.

TF risk presented by NPOs primarily arises in the context of sham charities, as distinct from legitimate charitable organizations. In the past several years, terrorist organizations have leveraged sham charities as a cover to raise funds. These sham charities are generally set up as foreign NPOs and may be established under the cover of providing humanitarian assistance but instead primarily or exclusively funnel money to a terrorist organization.

The Treasury Department is focused on identifying and designating sham charitable organizations, which reduces the overall TF risk of the NPO sector. For example, the Treasury Department has recently designated a number of sham charities.

- In 2023, Treasury imposed sanctions targeting Hamas-affiliated individuals and entities, including key Hamas officials and the mechanisms by which Iran provides support to Hamas and PIJ, such as through sham or fraudulent charitable organizations. Specifically, the Treasury designated the Gaza-based Al-Ansar Charity Association (Al-Ansar) and its director, Nasser Al Sheikh Ali, for serving as a conduit for illicit Iranian funds to Hamas and PIJ.[132]
- In 2023, Treasury also sanctioned the Muhjat Alquds Foundation in Gaza, a PIJ-run, Iran-funded organization whose primary mission is to provide financial support to the families of PIJ fighters and prisoners. Treasury also designated the leader of the Muhjat Alquds Foundation, PIJ political official Jamil Yusuf Ahmad 'Aliyan, who has distributed Iranian-provided funds to PIJ personnel in Gaza, has served on PIJ's executive committee, and has overseen PIJ finances as it relates to important group logistics.[133]

129 Department of the Treasury, OFAC, "Fact Sheet: Provision of Humanitarian Assistance and Trade to Combat COVID-19" (June 14, 2023), https://ofac.treasury.gov/media/931896/download?inline.

130 See U.S. Agency for International Development, Partner Vetting, https://www.usaid.gov/partner-vetting; see also U.S. Agency for International Development, "Annex 1- Risk Assessment and Management Plan For High-Risk Environments", https://2017-2020.usaid.gov/sites/default/files/documents/Annex_1_-_Risk_Assessment_and_Management_Plan_for_High-Risk_Environments.pdf.

131 The Department of the Treasury's De-Risking Strategy.

132 Treasury Press Release, "Treasury Targets Additional Sources of Support and Financing to Hamas," (October 27, 2023), https://home.treasury.gov/news/press-releases/jy1845.

133 Department of Treasury, OFAC, "United States and United Kingdom Take Coordinated Action Against Hamas Leaders and Financiers," (November 14, 2023), https://home.treasury.gov/news/press-releases/jy1907.

- In 2023, Treasury designated an environmentalist organization called Green Without Borders for providing support to, and collaborating with Hizballah in Lebanon.[134] Hizballah utilized outposts associated with Green Without Borders to hide weapons training and munitions tunnels, and thus provided cover to Hizballah's activities.[135]
- In 2022, the United States sanctioned a foreign NPO called World Human Care, established by the designated terrorist group Majelis Mujahidin Indonesia (MMI).[136] World Human Care did engage in some humanitarian activities, but the organization was established by MMI primarily to raise funds for its sympathizers in Syria.[137]

Fraudulent charitable appeals, without the involvement of a registered NPO, are the most common form of charitable abuse by terrorist groups. This method allows groups to cast a wide net to raise funds online, either through social media or dedicated crowdfunding websites (discussed in more detail below). This activity is difficult to detect and may result in individuals wittingly or unwittingly donating to a terrorist cause. This vulnerability is amplified by the fact that anyone can purport to raise money online using the pretext of a humanitarian cause, and the money must be tracked through to the end destination to be identified as funding terrorism.

Accordingly, although some NPOs have been misused to facilitate terrorist financing, Treasury and other U.S. government agencies note that the vast majority of U.S.-based tax-exempt charitable organizations face little or no risk of being abused for TF. This risk is substantially mitigated by the adoption of due diligence measures by charitable NPOs, Treasury's actions to identify and designate sham charitable organizations, and efforts to ensure NPOs have access to financial services.

EMERGING TRENDS

Crowdfunding & Online Fundraising

Crowdfunding and online fundraising are used domestically and transnationally for a variety of purposes including by charities or NPOs, business owners, and peer-to-peer exchanges.[138] The use of crowdfunding is substantial and growing: the global crowdfunding market is projected to reach $34.6 billion by 2026.[139] It involves many different actors, cross-border elements, and technological developments that can be exploited for TF purposes.[140] Notably, the majority of crowdfunding activity is legitimate. This status can make it more difficult for law enforcement attempting to investigate potential TF cases with a crowdfunding and online fundraising nexus. Compounding this issue, the anonymity, speed of transfers, and global reach of this method to collect and move funds make it an

134 Department of Treasury, OFAC, "Treasury Sanctions Lebanese Entity and Leader for Providing Support to Hizballah" (Aug. 16, 2023), https://home.treasury.gov/news/press-releases/jy1698.

135 Id.

136 Department of Treasury, OFAC, "Treasury Sanctions Organization Supporting Majelis Mujahidin Indonesia", (Feb. 3, 2022), https://home.treasury.gov/news/press-releases/jy0585.

137 Id.

138 See https://guides.loc.gov/small-business-financing/types/crowdfunding.

139 FATF Crowdfunding for TF Report, p. 10.

140 Id., p. 3.

attractive option for terrorist organizations.[141]

In the context of DVE, individuals who perpetrate attacks typically act alone or in a small group without seeking outside support or financing. Despite support voiced for these incidents, association is not a crime and thus donations to DVE or ideologically driven groups itself may not be sufficient cause for legal action. Further, some of the activities funded through these platforms may be constitutionally protected in the United States and would not be illegal unless tied to a specific act of violence or other unlawful act. As such, crowdfunding and online fundraising are typically legal activities employed to collect membership fees and fund programming. Over the past several years, DVEs and like-minded supporters have raised and moved millions of dollars using online crowdfunding platforms.[142]

Like domestic actors, international terrorist actors are successful in soliciting donations online. Terrorists continue to use encrypted apps like Telegram for communication as well as coordinating fundraising efforts, inhibiting law enforcement access to these communications. Also, fundraising campaigns often employ both fiat and virtual currencies, making it difficult to trace the origination of the transactions.

Crowdfunding through social media also represents a significant challenge for authorities. Online crowdfunding on these platforms can be done under the guise of legitimate charitable donations, making it difficult to identify as terrorist financing.[143] Vigilant monitoring is required to ensure illicit fundraising posts are quickly identified and taken down by social media companies. Further, some social media companies have now integrated their own payment mechanisms, creating another potential opportunity to transfer funds in support of terrorist activities. Additionally, the anonymity social media can provide a user can obscure the true identity of someone raising funds for illicit purposes.

Crowdfunding sees the convergence of many terrorist financing vulnerabilities: the overlap of social media, encrypted messaging platforms, peer-to-peer payments, virtual assets, and digitally enabled fundraising platforms. Utilizing more than one of these methods can obfuscate the source of funds or identity of the original transferrer. Many of these sectors are not required to apply AML/CFT measures as financial institutions, though they may intersect with an obligated entity at some point in the life cycle of the transaction.

141 Id.

142 See, e.g., ADL Crowdfunding Report: How Bigots and Extremists Collect and Use Millions in Online Donations | ADL.

143 See, for example, see FinCEN Alert, FIN-2023-Alert006, October 20, 2023 (identifying as a red flag indicator "A customer that is a charitable organization or nonprofit organization (NPO) solicits donations but does not appear to provide any charitable services or openly supports Hamas's terrorist activity or operations. In some cases, these organizations may post on social media platforms or encrypted messaging apps to solicit donations, including in virtual currency."

Conclusion

The terrorism and terrorist financing threat has evolved significantly since Treasury's first iteration of the TFRA in 2015. Terrorist organizations and violent extremist movements have shifted to a more diffuse, less hierarchical, networked structure facilitated by online communication, in which individuals may self-radicalize and become inspired by an ideology from across the globe. In the financing context, this means attacks by such radicalized individuals are smaller scale and require less outside financing, creating significant challenges for financial institutions and law enforcement looking to prevent attacks. However, terrorist organizations will still look to battle-tested methods of raising, moving, and using funds. As noted in the 2022 NTFRA, the threat of DVEs and financing of associated attacks continues to be the most pressing challenge for USG authorities.

While the world has seen significant successes in the past twenty-five years in the fight against the global scourge of terrorism, the October 7, 2023, Hamas attacks unambiguously demonstrated the awful consequences of underestimating the lethality of a group that has been developing a sophisticated financial enterprise in the background of other threats that were thought to be more acute. Even as new security challenges arise, terrorist adversaries adapt to our efforts, and new terrorist threats emerge around the world and here at home, the United States remains committed to evolving to meet this challenge and countering the next decade of terrorist threats.

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:

- **Department of Homeland Security**
  - Office of Strategy, Policy, and Plans,
    - Office of Counterterrorism Threat Prevention and Law Enforcement
- **Department of Justice (DOJ)**
  - Criminal Division
  - National Security Division
  - Federal Bureau of Investigation (FBI)
    - Counterterrorism Division
    - Criminal Investigative Division
- **Department of State (DOS)**
  - Bureau of Counterterrorism
- **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)
- **National Counterterrorism Center (NCTC)**
- **Staff of the Federal Functional Regulators**[144]

144 This includes staff of the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.

Methodology and Terminology

The terminology and methodology of the 2024 NTFRA are based on the guidance of the FATF, which is the international standard-setting body for anti-money laundering and countering the financing of terrorism (AML/CFT) safeguards. This guidance lays out a process for conducting a TF risk assessment at the national level.[145] The underlying concepts for this risk assessment are threats (the terrorists who are most active in raising or moving funds through the United States or U.S. financial system), vulnerabilities (weaknesses that facilitate TF), consequences (the effect of a vulnerability if successfully exploited by a threat), and risks (the synthesis of threat, vulnerability, and consequence). This approach uses the following key concepts:

- ***Threat:*** A threat is a person, a group of people, or 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, 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 2024 NTFRA focuses on threats and vulnerabilities in determining TF risks.
- ***Risk:*** Risk is a function of threat, vulnerability, and consequence. It represents a summary judgment, taking into consideration the effect of mitigating measures, including regulation, supervision, and enforcement.

The 2024 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, 2024.

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

List of Acronyms

AGAAVE	Anti-Government or Anti-Authority Violent Extremist
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
ANF	Al-Nusrah Front
AQ	al-Qa'ida
AQIM	al-Qa'ida in the Islamic Maghreb
BSA	Bank Secrecy Act
CBDC	Central Bank Digital Currency
CFTC	Commodity Futures Trading Commission
CVC	Convertible Virtual Currency
DHS	Department of Homeland Security
DOJ	Department of Justice
DVE	Domestic Violent Extremist
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCM	Future Commission Merchant
HTS	Hayat Tahrir al-Sham
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
MMI	Majelis Mujahidin Indonesia
MSB	Money Service Business
MVE	Militia Violent Extremist
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 Rulemaking
ODNI	Office of the Director of National Intelligence
OFAC	Office of Foreign Assets Control
P2P	Person-to-Person
PIJ	Palestinian Islamic Jihad
RIM	Russian Imperial Movement
RMVE	Racially or Ethnically Motivated Violent Extremist
SAR	Suspicious Activity Report
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