2022 National Terrorist Financing
Risk Assessment

February 2022

Department of the Treasury

2022 National Terrorist Financing
Risk Assessment

Table of Contents

Executive Summary

In the 20 years since the 9/11 attacks, the U.S. government, led by the Department of the Treasury (Treasury), has built a robust legal and institutional architecture to identify and disrupt terrorist financing (TF) domestically and internationally.

Domestically, this regime consists of legal authorities and investigative resources that prioritize identifying and prosecuting terrorist financiers, along with a robust U.S. anti-money laundering/countering-the-financing-of-terrorism (AML/CFT) framework. It is also supported by effective interagency information sharing and analysis, the collection and reporting on TF by financial institutions and other regulated entities, and regular information-sharing and engagement between the public and private sectors.

Internationally, Treasury, in coordination with the Departments of State (State), Justice (DOJ), and other interagency partners, works bilaterally to share typology and transactional information and to engage and build capacity so our foreign partners can take their own actions to dismantle TF networks and prevent terrorists' access to the international financial system. This has been complemented by work at key multilateral bodies to establish a global framework to combat TF, primarily through comprehensive international AML/CFT standards that help to prevent terrorists and other illicit actors from obscuring their activity in the international financial system. These activities have resulted in two important outcomes: (i) a clear global consensus that allowing designated terrorist groups to freely raise and move money through a country will have material consequences for that country (and others); and (ii) an international financial system that has become increasingly hostile to terrorists seeking to raise, move, and use funds.

Additionally, military operations have degraded al-Qa'ida's (AQ's) operational capabilities in some regions and dislodged the Islamic State of Iraq and Syria (ISIS) from urban centers in the Middle East. While ISIS and AQ seek to attack the United States, the risk of organized networks of operatives implementing complex plans developed by their leadership has decreased in recent years.

While we recognize these successes, the overall terrorist threat to the homeland from foreign terrorists persists, even if less acute than in previous years.[1] The foreign terrorist threat has become more ideologically diverse and geographically diffuse. We are also closely monitoring developments in Afghanistan and their potential impact on the terrorist and terrorist financing threats to the United States. One of the most significant developments in the U.S. terrorism landscape is the rising threat posed by domestic violent extremists (DVEs). DVEs espouse a range of violent ideological motivations, including racial or ethnic hatred as well as anti-government or anti-authority sentiment. This threat materializes in the form of lone actors, small groups of informally aligned individuals, networks exhorting and targeting violence toward specific communities, and violent self-proclaimed "militias."

Presently, the greatest threat to the homeland arises from U.S.-based individuals acting alone who, whether inspired by foreign groups or by ideologies that are more domestic in nature, act alone in carrying out deadly attacks, using firearms, vehicles, or homemade explosives.[2] These lone actors are increasingly reliant on their own personal finances to fund an attack, effectively separating any financial connection to terrorist organizations and

1 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, p. 23, (Apr. 9, 2021) (ODNI 2021 Threat Assessment).

2 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 global violent jihadist beliefs. HVEs are individuals inspired primarily by foreign terrorist groups, but who are not receiving individualized direction from those groups.

thus limiting the effect of certain AML/CFT measures at disrupting the financial aspects of terrorist activities. These individuals and those groups or networks that seek to inspire their violent acts exploit social media and encrypted communications to hide recruitment and radicalization to violence, and look to new financial products and services to obscure their transactional activity. 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.

Introduction

The 2022 National Terrorist Financing Risk Assessment (NTFRA) identifies the TF threats, vulnerabilities, and risks that the United States currently faces, updating the 2018 NTFRA.[3] This report, as well as the 2022 National Money Laundering Risk Assessment (NMLRA) and 2022 National Proliferation Financing Risk Assessment (NPFRA), provide an overview of the current illicit finance risks to the United States.

Terrorism remains a significant concern for the United States because terrorist groups at home and abroad still seek to conduct attacks inside the United States.[4] To counter these threats, Treasury focuses on disrupting the financial and support networks of these groups so they have access to fewer resources to develop and carry out attacks. Even as low-cost attacks by individuals inspired but not directed by terrorist groups have become more prominent, tracking and sharing financial information can still facilitate the disruption of such terrorist activity. The United States is particularly vulnerable to TF and other forms of illicit finance because much of the global economy touches the United States or the U.S. financial system, and the United States is the primary trading partner to many other countries. Trade transactions are often denominated in U.S. dollars and settled with a U.S. dollar-denominated funds transfer even if a U.S. customer is not a party to the transaction. In addition, U.S. currency is used globally as either the primary or de facto secondary reserve currency or store of value.

Participants

Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) drafted the 2022 NTFRA. The report incorporates published and unpublished research and analysis as well as the insights and observations of the managers and staff of the U.S. government agencies that reviewed the report:

- **Department of the Treasury**
  - Office of Terrorism and Financing 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
  - Internal Revenue Service (IRS)
    - Criminal Investigation (CI)
    - Tax Exempt & Government Entities Division (TEGE)
- **Department of Justice**
  - National Security Division
  - Criminal Division
  - Federal Bureau of Investigation (FBI)-Counterterrorism Division
  - Drug Enforcement Administration (DEA)
- **Department of Homeland Security (DHS)**
  - Homeland Security Investigations (HSI)

3 The 2018 NTFRA is available at https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf.

4 See ODNI 2021 Threat Assessment, p. 23.

- **Department of State**
  - Bureau of Counterterrorism
  - Bureau of Economic and Business Affairs
- **National Counterterrorism Center (NCTC)**
- **Staff of the federal functional regulators**[5]

Methodology

The terminology and methodology of the 2022 NTFRA are based on the guidance of the Financial Action Task Force (FATF), which is the international standard-setting body for AML/CFT safeguards. This guidance lays out a process for conducting a TF risk assessment at the national level.[6] 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), and risk (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.[7]
- Vulnerability: A vulnerability can be exploited to facilitate TF, both in the raising of funds for terrorist networks and the movement of funds to terrorists and terrorist organizations. It may relate to a specific financial product used to move funds or a weakness in regulation, supervision, or enforcement or reflect unique circumstances that may impact opportunities for terrorist financiers to raise or move funds or other assets.[8] 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.[9] Therefore the 2022 NTFRA focuses on threats and vulnerabilities in determining TF risks.
- Risk: Risk is a function of threat, vulnerability, and consequence.

The 2022 NTFRA relies on an analysis of criminal prosecutions,[10] Treasury designations, financial institution reporting, and other information available to the U.S. government,[11] along with a review of information on TF from international bodies such as the FATF and nongovernmental organizations. This information was used to

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

6 To assist in addressing some of the unique issues in TF, the FATF has issued specific guidance for assessing TF risk. See Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance* (TF Risk Assessment Guidance), (Jul. 2019), https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf.

7 Id., p. 8.

8 Id.

9 Id. As noted in the FATF TF Risk Assessment Guidance, given the challenges in assessing consequences, countries need not take a scientific approach when considering consequences, and instead may want to start with the presumption that consequences of TF will be severe (whether domestic or elsewhere) and consider whether there are any factors that would alter that conclusion.

10 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.

11 As with the 2018 NTFRA, the authors consulted classified sources of information to verify conclusions reached through a

determine (1) the terrorist groups that are most active in raising and moving funds through the United States and U.S. financial system, and the methods and typologies used by those groups to raise and move funds, and (2) which characteristics or circumstances of financial products, services, or market participants facilitate the raising or movement of funds by or on behalf of terrorists or terrorist organizations, and the extent to which domestic laws and regulations, law enforcement investigations and prosecutions, regulatory supervision, enforcement activity, and international outreach and coordination mitigate identified TF threats and vulnerabilities. This research and analysis were then used to identify the resulting TF risks facing the United States.

This 2022 NTFRA is divided into two sections: (1) threats and (2) vulnerabilities and the resulting TF risks.

consultation of information available in the public domain.

SECTION I. THREATS

Since the publication of the 2018 NTFRA, TF activity in the United States has evolved but largely continues to employ the same established methods for raising and moving funds. Funds moved from U.S.-based supporters to facilitators outside of the United States working on behalf of ISIS, AQ, and Hizballah remain the most common form of TF in the United States and this assessment focuses on these three foreign terrorist threats. However, the territorial defeat of ISIS in Iraq and Syria has affected the ways in which they provide financial support. Supporters of these groups are adapting to new technologies that can better obscure financial activities, while also decentralizing their operational structure to minimize the visible flow of funds.[12]

Additionally, the growing threat posed by DVEs has led to an increasing focus (and reporting) on financial activity associated with unlawful acts of force or violence by individuals and associated networks or movements involved in domestic violent extremism. Both domestic and foreign terrorist threats also seek to motivate individuals willing to launch an attack in the terrorists' name without formal training or support (including financial support).

For those individuals acting alone and for more organized terrorist networks, there are many ways to fund their activity. Contributions from individual supporters, including under the guise of charitable work, continue to provide a stable stream of revenue, and new technologies make it easier to anonymously raise funds through global crowdfunding programs. As the COVID-19 pandemic continues, these new payment technologies and systems have become a necessity rather than a convenience. Globally, proceeds generated from criminal activities such as corruption, extortion, drug and arms trafficking, and kidnapping for ransom remain a leading source of revenue for both terrorists and terrorist organizations writ large.

Islamic State of Iraq and Syria

According to the U.S. Intelligence Community's (IC) Annual Threat Assessment for 2021, ISIS remains capable of waging a prolonged insurgency in Iraq and Syria and leading a global organization and is still committed to attacking the United States and other Western nations.[13] International campaigns to counter ISIS have led to territorial losses, but the group continues to operate in Iraq, Syria, parts of Africa, South Asia, Southeast Asia, and elsewhere by capitalizing on corruption, poor governance, sectarianism, and economic malaise. During the past year, ISIS has had success in growing its presence across large swaths of Africa, as demonstrated by ISIS-Mozambique's temporary seizure in March of a coastal town where foreign workers on the country's largest liquefied natural gas project resided.[14] In Afghanistan, ISIS-Khorasan maintains a steady operational tempo and retains the ability to execute attacks in cities like Kabul.[15] Additionally, ISIS has reorganized and shifted to a decentralized structure that provides its branches and networks with more flexibility and independence, while allowing ISIS core leadership to be less visible. This new posture has allowed ISIS to sustain its influence—and in some areas around the globe, to expand it.

ISIS is best characterized as a global network of loosely organized branches and cells with varying financial activities coordinated under a central financial system that funds the core network and redistributes funds to

12 Financial Action Task Force, "Public Statement on the Financing of ISIL, Al Qaeda and Affiliates," (Oct. 2021), https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-isil-al-qaeda.html; Financial Action Task Force, "FATF Actions to Identify and Disrupt ISIL, Al-Qaeda and Affiliates' Financing," (Jun. 2019), https://www.fatf-gafi.org/publications/methodsandtrends/documents/fatf-action-against-terrorist-financing-june-2019.html.

13 ODNI 2021 Threat Assessment, p. 23.

14 See Testimony of NCTC Director Christine Abizaid, *Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11*, (Sep. 21, 2021) (NCTC 2021 Threat Testimony).

15 Id.

less wealthy affiliates or global regions that it sees as a priority.[16] In Iraq and Syria, ISIS has generated revenue through kidnapping for ransom, looting, and the extortion of local businesses, including payments from drug traffickers operating in ISIS-controlled strongholds. The group also leverages their support network within refugee camps, such as al-Hawl in Northern Syria and others, to receive donations from supporters in the international community. External donations to refugee camps come into the region through various means—such as money remitters and virtual asset service providers (VASPs) —and then exit the regulated financial system as cash via hawaladars, where they are subsequently sent to the camp. To solicit donations, ISIS supporters in these camps often use various social media platforms and disguise their appeal as humanitarian aid. In Africa, extortion and kidnapping for ransom remain key sources of funding for ISIS, but recent reports also indicate that revenues from the extortion of artisanal gold mining-related activities is increasing.[17] Virtual assets are being sent directly to ISIS supporters located in northern Syria, often to Idlib, or indirectly via Turkey, where ISIS is able to access them at virtual asset trading platforms.[18]

In addition to revenue generated from its illicit financial activities, as of late 2020, ISIS also had access to an estimated $25-50 million in cash reserves dispersed across Iraq and Syria.[19] Reserves have primarily come from the sale of oil, the "taxation" of local populations under ISIS's former territorial control in Iraq and Syria, and cash seizures, such as ISIS's 2014 theft of hundreds of millions in cash reserves from Iraqi banks in Mosul. ISIS's largest expenditures are the salaries it pays fighters and payments to families of imprisoned or deceased fighters. In Syria and Iraq, ISIS primarily spends its funds on salaries and stipends for its members (including families of deceased fighters) and on supporting operational activities (e.g., food, clothing, arms, training, and propaganda). ISIS also continues to use networks of couriers to smuggle cash between and among Iraq, Syria, and Turkey. To transfer funds outside the region, the group also relies on financial facilitation networks that use money remitters often located in regional financial and logistical hubs, such as Turkey and the United Arab Emirates (UAE).

In the United States, financial activity involving ISIS continues to primarily involve individual ISIS supporters who use their personal savings either to fund a would-be fighter's travel to conflict zones or to send funds to financial facilitators who consolidate and then forward these funds to foreign shell companies or individual ISIS operatives outside the conflict zone, who are often unbeknownst to the relevant financial institutions.[20] In these instances, most funds have been generated from legal activity or sources such as accessing credit, personal savings, or selling assets, although a few have involved generating funds from criminal activity (most of which was nonviolent).[21]

- In September 2021, a married couple pleaded guilty and were sentenced to 18 months and two years in prison, respectively, for conspiring to provide material support and resources to ISIS. They provided and attempted to provide financial support to two relatives for the purpose of traveling to Syria to join ISIS fighters.[22]
- In October 2021, an individual pleaded guilty to attempting to provide material support and resources to ISIS and Al-Nusrah Front (ANF). According to court documents, the individual, like his co-conspirators, was

16 Department of State, "The United States Designates ISIS Financial Facilitators," (May 17, 2021), https://www.state.gov/the-united-states-designates-isis-financial-facilitators/.

17 International Crisis Group, *The Islamic State Franchises in Africa: Lessons from Lake Chad*, (Oct. 29, 2020), https://www.crisisgroup.org/africa/west-africa/nigeria/islamic-state-franchises-africa-lessons-lake-chad.

18 *U.S. v. Facemaskcenter.com and Four Facebook Pages*, (Complaint for Forfeiture In Rem) (D.D.C., Aug. 5, 2020).

19 UN Analytical Support and Sanctions Monitoring Team, *28th Report of Analytical Support and Sanctions Monitoring Team*, p. 33, (Jul. 21, 2021) (28th UN MT Report), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2021_655_E.pdf.

20 George Washington University, Program on Extremism, *Dollars for Daesh: Analyzing the Finances of American ISIS Supporters*, p. 6, (Sep. 2020), (Dollars for Daesh Report), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Dollars%20for%20Daesh%20final%20report.pdf

21 Id.

22 Department of Justice, "Bangladeshi Husband and Wife Sentenced For Conspiring to Provide Material Support to ISIS," (Sep. 9,

a member of a domestic support network for individuals who sought to travel to the Middle East to join ISIS or ANF. He donated his own money, and he worked with his co-conspirators to raise money from others that was intended to be used to help other individuals to travel to Syria to join and fight on behalf of ISIS or ANF. In particular, in February 2015, the individual arranged for money to be deposited into the bank account of another member of the network before that individual attempted to leave for Syria.[23]

- In August 2020, DOJ announced a series of forfeiture actions to dismantle several cyber-enabled terror finance campaigns supporting ISIS, AQ, and HAMAS.[24] The ISIS-related criminal complaint highlighted an alleged scheme by an ISIS facilitator who was responsible for managing select ISIS hacking operations to sell fake personal protective equipment via FaceMaskCenter.com. Site administrators claimed to have near unlimited supplies of N95 respirator masks, in spite of such items being officially designated as scarce. The site administrators offered to sell these items to customers across the globe, including a customer in the United States who sought to purchase N95 masks and other protective equipment for hospitals, nursing homes, and fire departments.

While ISIS remains the foreign terrorist group most frequently involved in TF activity in the United States[25], there has been a significant reduction in the number of U.S. persons traveling overseas to join ISIS in Iraq and Syria, likely due to the impact of the counter-ISIS campaign in Iraq and Syria.[26] However, it is also possible that U.S. persons seeking to join or fund ISIS have shifted their efforts to join or support ISIS branches and networks in parts of Africa, South Asia, and Southeast Asia, where the group remains active.

To move funds, some reports indicate that U.S.-based ISIS supporters collect and consolidate donations within the United States and then transfer funds outside of the United States using unwitting money services businesses (MSBs) rather than unwitting banks. ISIS's use of virtual assets remains limited, as do direct financial exchanges between U.S. persons and known ISIS supporters.[27] The infrequency or inconsistency and small dollar amounts of these donations and the indirect relationship between U.S.-based ISIS supporters and ISIS operatives remain the biggest challenge for financial institutions to detect this activity proactively.

Along with raising relatively small amounts of funds from U.S.-based supporters, ISIS financial facilitators are looking for ways to move funds raised in the United States to shell companies around the world.[28] This system creates layers between U.S.-based supporters and ISIS, allowing the transactions to circumvent monitoring by financial institutions. U.S. authorities have identified instances where ISIS operatives route transactions through complicit individuals, and in some instances shell companies and other legal entities, to avoid detection. They also channel financial activity through neighboring localities (as ISIS operates in regions with limited access to the international financial system).[29] This leaves U.S. financial institutions at risk of unwittingly enabling TF, either

---

2021), https://www.justice.gov/usao-edpa/pr/bangladeshi-husband-and-wife-sentenced-conspiring-provide-material-support-isis.

23 Department of Justice, "Man Pleads Guilty to Attempting to Provide Material Support to ISIS and Al-Nusra Front," (Oct. 18, 2021), https://www.justice.gov/opa/pr/man-pleads-guilty-attempting-provide-material-support-isis-and-al-nusra-front.

24 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," (Aug. 13. 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

25 The case examples above involve activities conducted in 2015 but are nonetheless instructive of the typical financial activity used to finance or facilitate travel for individuals seeking to join terrorist movements overseas.

26 Department of State, *Country Reports on Terrorism 2019*, https://www.state.gov/reports/country-reports-on-terrorism-2019/.

27 See Dollars for Daesh Report, pp. 7, 33.

28 See, for example, *U.S. v. Zoobia Shahnaz* (the defendant executed several wire transactions totaling over $150,000 to individuals and shell entities in Pakistan, China, and Turkey that were fronts for ISIS). Department of Justice, "New York Woman Pleads Guilty to Providing Material Support to ISIS," (Nov. 26, 2018), https://www.justice.gov/opa/pr/new-york-woman-pleads-guilty-providing-material-support-isis.

29 See, for example, Department of the Treasury, OFAC, "Treasury Targets ISIS Financial Facilitators in Syria and Turkey," (May 17, 2021), https://home.treasury.gov/news/press-releases/jy0179.

directly or through their correspondent relationships.

U.S. authorities continue to identify complicit foreign money remitters and exchange houses that have assisted ISIS in accessing the international financial system. For example, in May 2021, Treasury designated Turkey-based Al-Fay Company, two of its managers, and another Turkey-based MSB operator for facilitating ISIS funds transfers.[30] In September and November 2019, Treasury designated a range of other Turkey- and Syria-based MSBs and their operators for providing financial support to ISIS.[31] As of late 2021, Turkish authorities announced asset freezes against ISIS financial facilitators, who were designated by the United States between 2019 and 2021, but the practical impact of Turkish actions is largely unclear. Additionally, as noted in the 2018 NTFRA, ISIS supporters may transfer funds through foreign financial institutions that are not subject to the same or similar regulatory requirements as U.S. financial institutions, and thus do not have in place effective AML/CFT processes or controls.

Al-Qa'ida

According to the IC, AQ's senior leadership has suffered severe losses in the past few years, but remaining leaders in the Middle East, Africa, and Asia encourage cooperation among decentralized regional elements and continue to call on them to attack the United States and other international targets.[32] AQ's regional affiliates continue to exploit local conflicts and ungoverned spaces to threaten U.S. and other Western interests, as well as local governments and populations abroad.

Unregistered money remitters remain one of AQ's most prevalent means to transfer funds.[33] AQ also continues to exploit access to the regulated financial system to support its ongoing terrorist activities. Like ISIS, AQ has sought out non-U.S. financial institutions that are subject to less rigorous regulatory oversight and used them to transfer funds. For example, a September 2021 Treasury designation identified a network of Turkey-based AQ financial facilitators who moved funds, including via couriers, to militants in conflict zones, such as Syria, as well as to AQ leadership.[34] This network facilitated electronic and cash transfers and provided funds to the families of imprisoned AQ members. Turkish authorities have yet to announce any disruptive actions against this AQ network, although in November 2021, the Turkish government ordered an asset freeze targeting a separate Turkey-based AQ financial facilitator, Hasan al-Shaban, who was designated by Treasury in July 2021.[35]

In another example, as of mid-2021, Hasan al-Shaban was using his Turkish bank account to receive and consolidate donations to AQ from associates across North Africa, Western Europe, and North America and separately used the account to coordinate the transfer of funds to Turkey. The money was then used to support AQ terrorist operations in Syria.[36]

30 Id.

31 Department of the Treasury, OFAC, "Treasury Designates ISIS Financial, Procurement, and Recruitment Networks in the Middle East and South Asia," (Nov. 18, 2019), https://home.treasury.gov/news/press-releases/sm831.

32 ODNI 2021 Threat Assessment, p. 23.

33 28th UN MT Report, p. 18.

34 Department of the Treasury, OFAC, "Treasury Designates al-Qa'ida Financial Network in Turkey," (Sep. 16, 2021), https://home.treasury.gov/news/press-releases/jy0358.

35 Associated Press, *Turkey freezes assets of 770 people for alleged terror link*, (Dec. 24, 2021), https://apnews.com/article/business-islamic-state-group-fethullah-gulen-14097fef97c988cb331c177e73b3a642.

36 Department of the Treasury, OFAC, "Treasury Designates Al-Qa'ida-Linked Financial Facilitators in Turkey and Syria," (July 28, 2021), https://home.treasury.gov/news/press-releases/jy0293.

AQ also leverages seemingly licit business activity to support its financial activities. Prior to his arrest by Australian authorities on terrorism-related charges,[37] AQ financial facilitator Ahmed Luqman Talib conducted financial transactions in several countries, including dealing in gemstones, allowing him to move funds and individuals internationally for the benefit of AQ.[38] Talib conducted business around the world, including in Brazil, Colombia, Sri Lanka, Tanzania, Turkey, and the Gulf.[39]

Some AQ facilitators have also set up front or sham charities or solicited donations under the guise of charitable causes and are continuing to explore raising and moving funds in virtual assets. In August 2020, DOJ announced the dismantling of a cyber-enabled AQ financing campaign largely based out of Syria.[40] AQ and the affiliated groups operated a bitcoin ML network using Telegram channels and other social media platforms to solicit virtual asset donations.[41] In some instances, they purported to act as charities when, in fact, they were openly and explicitly soliciting funds for violent terrorist attacks.[42] One solicitation on behalf of Al Sadaqah ("charity" in Arabic) sought virtual asset donations to equip terrorists in Syria with weapons.[43] The scheme operators used complicated obfuscation techniques, layering transactions to conceal their actions.[44]

In late 2020, French authorities prosecuted eight people for their alleged involvement in a complex scheme financing Islamic extremists, including AQ, in Syria through the use of virtual assets.[45] Active since 2019, the network was thought to have supplied hundreds of thousands of Euros via the scheme, based mainly on the purchase in France of virtual asset vouchers, details of which were transferred by secure messaging to jihadis in Syria, who could then retrieve the money through virtual asset trading platforms.[46] In 2021, AQ also published a bounty offer for the killing of police officers with the reward to be paid in bitcoin.[47] While the activity in these cases did not occur in the United States, it is representative of the exploitation that may occur in the U.S. financial system.

AQ affiliates operating in regions with weak governance exploit control over territory to generate funds. These include AQ affiliate Jama'a Nusrat ul-Islam wa al-Muslimin, which is active in West Africa; al-Shabaab in Somalia and other east African countries; and formerly AQ-aligned Hay'at Tahrir al-Sham (HTS), which remains the predominant terrorist group in northwestern Syria. HTS raises revenue from taxation and levies and recently introduced fees for building permits and increased taxes imposed on telecommunications service providers.[48]

---

37 The Sydney Morning Herald, *Australian jihadists engaged in fierce Syrian battle with help of gemstone dealer: police*, (May 1, 2021), https://www.smh.com.au/national/australian-jihadists-engaged-in-fierce-syrian-battle-with-help-of-gemstone-dealer-police-20210428-p57n6x.html#:~:text=Ahmed%20Luqman%20Talib%2C%20who%20runs,to%20engage%20in%20hostile%20activities.

38 Department of the Treasury, OFAC, "Treasury Designates al-Qa'ida Financial Facilitator," (Oct. 19, 2020), https://home.treasury.gov/news/press-releases/sm1157.

39 Id.

40 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," (Aug. 13, 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

41 Id.

42 Id.

43 Id.

44 Id.

45 UN Analytical Support and Sanctions Monitoring Team, *27th Report of Analytical Support and Sanctions Monitoring Team*, p. 18, (Jan. 21, 2021) (27th UN MT Report), https://undocs.org/S/2021/68; see also Associated Press, *8 Charged in French Cryptocurrency Scheme to Finance Jihadis*, (Oct. 3, 2020), https://apnews.com/article/technology-cryptocurrency-terrorism-archive-france-784cfaa3a2e272ff1cf3b4c5d1dc9a6a.

46 Id.

47 The Arab Weekly, *Jihadist magazine offered $60,000 bounty for the killing of Western police officer*, (May 6, 2021), https://thearabweekly.com/jihadist-magazine-offered-60000-bounty-killing-western-police-officer.

48 27th UN MT Report, p. 11.

Within the United States, AQ's financial footprint involves funds sent by individual supporters or through charitable front organizations to AQ operatives or facilitators overseas.

In July 2020, an individual was arrested for attempting to provide material support to AQ. The individual allegedly gave a purported AQ member a $500 prepaid gift card to purchase scopes for rifles that would be used by AQ members to kill American soldiers. According to the criminal complaint, the individual decided to see if they could buy a card at a local store in order to conceal their identity (because buying one online requires the disclosure of personal information). The individual also purchased airline tickets for personal travel to Afghanistan to join AQ.

In September 2019, an individual pleaded guilty to concealing the financing of terrorism.[49] According to the criminal complaint, the individual instructed an undercover federal employee on how to send money to fighters engaged in jihad in a manner that would avoid detection by law enforcement and customer identification requirements imposed by the money transmitter, such as using fake names and addresses when conducting electronic money transfers.[50] Subsequently, the individual introduced the undercover agent to a financial facilitator who could route money to AQ.

Hizballah

Hizballah has long been involved in conducting and directing a range of military, terrorist, criminal, and other illicit activities globally. Hizballah maintains the capability to target, both directly and indirectly, U.S. interests inside Lebanon, in the Middle East, in other overseas locations, and—to a lesser extent—in the United States.[51] To bolster its military and terrorist capabilities, Hizballah maintains an international financing and procurement network,[52] with front companies around the world.[53] Hizballah's main source of financial support is Iran, which provides hundreds of millions of dollars per year.[54] Hizballah also receives financial support from some members of Lebanese diaspora communities.[55] Along with banks, money exchange houses and unregulated cash-based networks in South America have been used to move money from Hizballah supporters and facilitators in the Lebanese diaspora community to support Hizballah's violent operations in Lebanon, Syria, and elsewhere.

Hizballah financiers and sympathizers also take advantage of free trade zones and countries with weak regulatory environments to establish import-export companies and execute complex trade-based ML schemes that move money to China, the United States, and elsewhere. Hizballah and suspected Hizballah financiers have operated businesses in free trade zones for years, including the Tri-Border Area of Argentina, Brazil, and Paraguay; the Free Zone of Iquique in Chile; and the Colon Free Trade Zone in Panama.[56]

---

49 Department of Justice, "Former Alabama Resident Pleads Guilty to Concealing Terrorism Financing," (Sep. 13, 2019), https://www.justice.gov/opa/pr/former-alabama-resident-pleads-guilty-concealing-terrorism-financing.

50 Id.; *U.S. v. Alaa Mohd Abusaad* (Criminal Complaint) (N.D. Al. Oct. 22, 2018).

51 ODNI 2021 Threat Assessment, p. 24.

52 Department of Justice, "Lebanese Businessman Tied by Treasury Department to Hezbollah is Sentenced to Prison for Money Laundering Scheme Involving the Evasion of U.S. Sanctions," (Aug. 8, 2019), https://www.justice.gov/opa/pr/lebanese-businessman-tied-treasury-department-hezbollah-sentenced-prison-money-laundering.

53 Department of the Treasury, OFAC, "Treasury Designates Prominent Lebanon and DRC-Based Hizballah Money Launderers," (Dec. 13, 2019), https://home.treasury.gov/news/press-releases/sm856.

54 Under Secretary for Terrorism and Financial Crimes Sigal Mandelker, *Speech before the Foundation for the Defense of Democracies*, (Jun. 5, 2018), https://home.treasury.gov/news/press-releases/sm0406.

55 See Testimony of Assistant Secretary for Terrorist Financing and Financial Crimes Daniel Glaser, (Jun. 9, 2016). https://www.treasury.gov/press-center/press-releases/Pages/jl0486.aspx

56 Department of Justice, "Two Men Arrested for Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," (Jun. 8, 2017), https://www.justice.gov/opa/pr/two-men-arrested-terrorist-activities-behalf-hizballahs-islamic-jihad-organization; Department of Justice, "Alleged Supporter of Terrorist Group Extradited from Paraguay," (Feb. 25, 2011), https://archives.fbi.

Mahmoud Barakat and Nader Farhat are examples of Hizballah financiers who operated out of the Tri-Border Area. Farhat operated one of the biggest currency exchange businesses in the region, Cambios Unique S.A., before his arrest and extradition to the United States on ML charges in a DEA investigation.[57] As is common for many criminals, including drug traffickers and terrorist financiers, Farhat's company was and continues to be held in the name of a relative—his wife—distancing his name from the company in an attempt to avoid detection and disruption.

Hizballah members, supporters, and sympathizers are involved to varying degrees in a broad range of large-scale criminal schemes around the world, including ML, fraud, counterfeiting, narcotics trafficking, and weapons procurement. For example, on April 11, 2019, Treasury designated prominent Hizballah money launderer Kassem Chams and his international ML network for moving tens of millions of dollars a month in illicit narcotics proceeds on behalf of drug kingpins such as the Colombian criminal group, La Oficina De Envigado, and using the profits to finance Hizballah.[58] ML networks like Chams's show that Hizballah relies on financial facilitators who provide ML services to unrelated criminal organizations.

Additionally, on December 13, 2019, Treasury designated prominent Hizballah money launderers Nazem Said Ahmad and Saleh Assi. As of late 2016, Ahmad was considered a major Hizballah financial donor who used his family's Africa-based diamond businesses to launder money into Lebanon on behalf of Hizballah Secretary General Hassan Nasrallah.[59] Assi and entities he controlled engaged in tax evasion and ML schemes in the Democratic Republic of the Congo that generated tens of millions of dollars per year, a portion of which was transferred to U.S.-designated Hizballah financier Adham Husayn Tabaja in Lebanon via bulk cash transfers or laundered through entities associated with Nazim Ahmad's diamond business.[60]

Iran has reduced its financial support to Hizballah, largely due to Iran's ongoing economic difficulties and U.S. sanctions, leaving the organization financially strained and seeking alternative sources of funding.[61] This could include greater reliance on the proceeds of illicit activity and pressuring Hizballah-linked individuals and entities to increase their revenues.

Within the United States, Hizballah supporters continue to be financially active, including through criminal activity. In May 2021, a dual Lebanese and U.S. citizen pleaded guilty to participating in a conspiracy to launder money as part of a decade-long Hizballah scheme to ship electronics equipment to a Hizballah-owned television station in Lebanon.[62] According to court documents, the defendant received money from an unindicted co-conspirator in Lebanon, which the defendant used to purchase electronics equipment in the United States. She then shipped the items purchased by herself and other co-conspirators overseas, primarily to Lebanon, where the unindicted co-conspirator supplied at least $175,000 worth of goods to the television station.

The global reach and involvement of Hizballah supporters and facilitators in a range of legal commerce and illegal

---

gov/archives/philadelphia/press-releases/2011/ph022511a.htm.

57 *U.S. v. Nader Mohamad Farhat et al* (Indictment) (S.D. Fla. Nov. 21, 2019).

58 Department of the Treasury, OFAC, "Treasury Sanctions Lebanese Money Launderer Kassem Chams Who Moves Money on Behalf of Narcotics Trafficking Organizations and Hizballah," (Apr. 11, 2019), https://home.treasury.gov/news/press-releases/sm650.

59 Department of the Treasury, OFAC, "Treasury Designates Prominent Lebanon and DRC-Based Hizballah Money Launderers," (Dec. 13, 2019), https://home.treasury.gov/news/press-releases/sm856.

60 Id.

61 Remarks by Assistant Secretary Marshall Billingslea on Hizballah and Iran's Financial Networks, (Sep. 13, 2019), https://home.treasury.gov/news/press-releases/sm776.

62 Department of Justice, "Dual Lebanese-U.S. Citizen Pleads Guilty to Money Laundering and Tax Offenses," (May 10, 2021), https://www.justice.gov/usao-edva/pr/dual-lebanese-us-citizen-pleads-guilty-money-laundering-and-tax-offenses.

activities that often involve access to the banking system means it is more likely that Hizballah-linked funds may come through U.S. banks compared to other terrorist groups that rely on money remitters as their point of entry into the financial system. Further, while most U.S.-based individuals supporting jihadist terrorist networks engage in outbound transfers or use funds to facilitate travel, Hizballah supporters are more likely to send funds into the U.S. or transit the U.S. financial system for transactions between a non-U.S. originator and recipient.

Other Foreign Terrorist Groups

Other foreign terrorist threats may seek to raise, use, or move funds in the United States or through the U.S. financial system but are less active than the three groups identified above. These include Lashkar-e-Tayyiba (LeT), HAMAS, as well as other jihadist groups active in Africa, the Middle East, Asia, and South America.

Treasury and its interagency partners continue to closely monitor the situation in Afghanistan and its repercussions for terrorism and its financing. ISIS and AQ affiliates, such as ISIS-Khorasan, are present in Afghanistan. These groups could seek to raise funds through tactics including extortion, kidnapping for ransom, or drug trafficking, as other terrorist groups active in Afghanistan have done. These funds could be used to support their own activities and those of ISIS and AQ branches and affiliates around the world. There is also the possibility that, depending on the intensity of the conflict there, some U.S. persons may travel to Afghanistan and join ISIS, AQ, or other terrorist groups such as the Haqqani network, or seek to provide these groups with financial support.[63]

Domestic Violent Extremism

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.[64] This risk assessment, as well as the law enforcement and IC assessments it references, do not include individuals engaged solely in activities protected by the First Amendment or other rights secured by the U.S. Constitution.[65]

U.S. authorities categorize DVEs based on the ideology motivating their violent conduct. For example, racially or ethnically motivated violent extremists (RMVEs) are individuals motivated by bias, often related to race or ethnicity, held by the actor against others or a given population group. Another category of DVE threat is anti-government or anti-authority violent extremists. These individuals are motivated by anti-government or anti-authority sentiment, including opposition to perceived economic, social, or racial hierarchies, or perceived government overreach, negligence, or illegitimacy.[66]

As noted in the 2021 *National Strategy for Countering Domestic Terrorism*, DVEs pose a serious and evolving threat.[67] Since the spring of 2020, for example, the FBI has more than doubled the number of its DVE investigations, from

63 For instance, in October 2021, a U.S. individual was found guilty for attempting to provide material support for terrorism and attempting to make a contribution of funds, goods, and services to the Taliban. Department of Justice, "Bronx Man Who Attempted To Travel To Afghanistan In 2019 To Join Taliban Convicted Of Attempting To Provide Material Support For Terrorism," (Oct. 11, 2021), https://www.justice.gov/usao-sdny/pr/bronx-man-who-attempted-travel-afghanistan-2019-join-taliban-convicted-attempting.

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

65 As the IC has noted: "Mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute violent extremism, and may be constitutionally protected." ODNI DVE Assessment at 4.

66 See ODNI DVE Assessment, p. 4 for additional information on how the U.S. government classifies the ideologies motivating various DVE threats.

67 The White House, *National Strategy for Countering Domestic Terrorism*, (June 2021).

about 1,000 to around 2,700.[68] Earlier this year, the intelligence and law enforcement communities conducted a comprehensive assessment of the DVE threat and found that DVEs motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the United States.[69]

The IC assesses that lone offenders or small cells of DVEs adhering to a diverse set of violent extremist ideologies are more likely to carry out violent attacks in the United States than larger organizations that allegedly advocate a DVE ideology. The IC notes that DVE attackers often radicalize independently by consuming violent extremist material online and mobilize without direction from a violent extremist organization, making detection and disruption difficult. In 2021, the IC has assessed that RMVEs and militia violent extremists (MVEs) present the most lethal DVE threats, RMVEs being most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement and government personnel and facilities.[70]

Self-financing (usually through employment income or savings) is a significant source of funds for DVEs. This presents a challenge for financial institutions because the transactional activity is unlikely to look different than the customer's expected activity, based on risk profile. Additionally, DVEs can use a number of generally licit means to fundraise for their illicit activity. Such methods can include crowdfunding (which allows DVEs to cast a wide net via internet platforms like social media and gaming chatrooms); private donations and membership fees (which are sometimes transacted through virtual assets, making it challenging for authorities to detect); and commercial activities such as the sale of merchandise or entertainment events.[71] Some of these activities may be protected by the First Amendment to the U.S. Constitution.[72] However, DVEs also use a variety of other illicit methods to generate revenue to fund their illicit activity. For example, some DVEs have used theft, fraud, and drug trafficking to generate revenue.[73]

DVE attacks are sometimes carried out by individuals with a low-risk financial profile. For example, their funds may be raised from legal sources, may generally be spent on legal activities, may not touch a high-risk jurisdiction, and they may not have identifiable ties to a designated individual terrorist or organization. This is one of the reasons that the movement of DVE funds can be difficult to detect prior to an attack, arrest, or the emergence of other derogatory information about the transaction parties, and why combating DVE financing presents a particular challenge. According to a June 2021 FATF report, foreign groups with similar ideologies and structures tend to move funds through person-to-person transfers, cash transactions, and in some cases, virtual asset transfers.[74] U.S. authorities have identified financial activity indicating that some extremist groups may be seeking to purchase property so they can facilitate paramilitary-style training, to include learning how to make improvised explosive devices, for members or other like-minded individuals.

- For example, "The Base" is a violent extremist group whose members have discussed, among other things, creating a white ethno-state, committing acts of violence against minority communities, organizing military-

68 Testimony of FBI Director Christopher Wray, *Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11*, (Sep. 21, 2021).

69 See ODNI DVE Assessment, p. 2.

70 Id.

71 See Financial Action Task Force, Ethnically or Racially-Motivated Terrorist Financing, pp. 8, 11, 14 (Jun. 2021) (FATF REMT Report), https://www.fatf-gafi.org/media/fatf/documents/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf.

72 "Mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute violent extremism, and may be constitutionally protected." ODNI DVE Assessment at 4.

73 See, for example, Department of Justice, "Five Men Associated With The Aryan Brotherhood Indicted For Illegal Possession And Transfer Of Firearms And Conspiracy To Distribute Methamphetamine," (Apr. 28, 2017), https://www.justice.gov/usao-mdpa/pr/five-men-associated-aryan-brotherhood-indicted-illegal-possession-and-transfer-firearms.

74 FATF REMT Report, p. 21.

style training camps, and manufacturing improvised explosive devices. In June 2021, two members of "The Base" pleaded guilty to firearms and immigration-related criminal charges. A third member previously pleaded guilty to conspiring to transport an alien and was sentenced to five years in prison and three years of supervised release.[75] According to court filings, the three individuals were planning violence at an upcoming political rally and expressed hope that bloodshed could start a civil war.[76] According to other court filings, in addition to communicating with other members of "The Base," the individuals made several purchases of ammunition and firearms accessories and engaged in tactical training at military-style training camps in the U.S. state of Georgia with connections to "The Base."[77]

Additionally, U.S. law enforcement officials have also been tracking the growing number of transnational connections between RMVEs, including links between groups in the United States and abroad individuals and groups.[78] This global phenomenon includes RMVE and like-minded networks in the United States, Canada, South America, Europe, Russia, South Africa, New Zealand, and Australia.[79] According to the IC, U.S.-based RMVEs who promote the superiority of the white race have the most persistent and concerning transnational connections because individuals with similar ideological beliefs exist outside of the United States, and these RMVEs frequently communicate with and seek to influence each other.[80]

The IC assesses that a small number of U.S. RMVEs have traveled abroad to network with like-minded individuals.[81] In some instances, RMVEs have traveled to participate in paramilitary or other specialized training.[82] This also can include travel to Syria and Iraq to join groups fighting ISIS (sometimes, specifically to protect Christian minorities), as well as the conflict in Ukraine.[83] While there have been limited identified financial connections between these groups, they may seek stronger cross-border financial ties as they continue to interact.

75 Department of Justice, "Two Members of the Violent Extremist Group "The Base" Plead Guilty to Federal Firearms and Alien-Related Charges," (Jun. 10, 2021), https://www.justice.gov/usao-md/pr/two-members-violent-extremist-group-base-plead-guilty-federal-firearms-and-alien-related; *U.S. v. Brian Mark Lemley Jr. et al* (Motion for Detention Pending Trial) (D. Md. Jan. 21, 2020).

76 Id., p. 11.

77 Id., pp. 16, 17, and 24.

78 ODNI DVE Assessment, p. 2.

79 See Financial Action Task Force, *Ethnically or Racially-Motivated Terrorist Financing*, Annex A (Jun. 2021) (FATF REMT Report at Annex A.), https://www.fatf-gafi.org/media/fatf/documents/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf.

80 ODNI DVE Assessment, p. 2.

81 Id.

82 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

83 FATF REMT Report pp. 35-36.

SECTION II. VULNERABILITIES AND RISKS

Since 9/11, U.S. authorities have made significant progress in addressing some of the key vulnerabilities that AQ and other terrorist groups have been able to exploit. By developing deep expertise on TF threats and vulnerabilities, building a robust legal and operational architecture, and strengthening international relationships and institutions, the United States has degraded the financial and support networks for a range of terrorist groups. For example, FinCEN and U.S. law enforcement undertook a coordinated effort to target individuals or businesses operating as unlicensed money transmitters, which AQ had exploited to fund operatives around the world.[84]

Treasury, along with its interagency and foreign partners, has worked collaboratively with charitable organizations to strengthen their internal measures and requirements so they are much less likely to be exploited by terrorist groups for fundraising or facilitation activities. Moreover, the USA PATRIOT Act created a legal framework for the U.S. government to share information and help financial institutions better identify and report TF activity, as well as for financial institutions to share information among themselves when they have a reasonable basis to believe that the information shared relates to activities that may involve terrorist activity or ML.[85] Recent amendments have strengthened that legal framework.[86] However, those responsible for safeguarding the U.S. financial system continue to face challenges in countering TF as terrorists and terrorist financiers adapt. These include the difficulty in distinguishing terrorist-related financial activity from licit financial flows, as well as continuing weaknesses in the AML/CFT regimes of certain foreign financial systems that some terrorist groups exploit as an entry point into the international financial system.

Banks

While innovations in financial technology and changes in consumer preferences continue to create new options for Americans seeking to transfer money at home and overseas, banks remain the primary channels by which U.S. persons and businesses transfer funds domestically and internationally. Almost 95 percent of U.S. households (approximately 124 million) had a bank or credit union account in 2021.[87] Further, automated clearing house payments accounted for 66.1 percent of the value of all noncash payments in 2018.[88]

Along with their robust domestic presence, U.S. banks process trillions of dollars of global transactions per day for domestic and foreign customers. The significant volume of funds moved globally each day can allow terrorist-related transactions to blend in with other licit transactions. In response to this risk, many U.S banks have developed sophisticated transaction monitoring systems and other approaches to identify and report financial activity linked to known and previously unknown terrorist operatives. Thus, while U.S. banks remain one of the primary avenues by which terrorist groups attempt to move funds in or through the United States, the visibility provided by this monitoring and associated suspicious activity reporting helps law enforcement prevent and detect TF.

84 Department of the Treasury, *National Terrorist Financing Risk Assessment*, p. 54 (Jun. 12, 2015), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

85 FinCEN, *Section 314 (b) Fact Sheet*, (Dec. 1, 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

86 See FinCEN, Anti-Money Laundering Act of 2020, Sections 6206, 6212, and 6214, https://www.fincen.gov/anti-money-laundering-act-2020.

87 Federal Deposit Insurance Corporation, *How America Banks: Household Use of Banking and Financial Services (2019)*, (Oct. 2020) (2019 FDIC Household Banking Survey), https://www.fdic.gov/analysis/household-survey/index.html.

88 Board of Governors of the Federal Reserve System, *The 2019 Federal Reserve Payments Study*, (Jan. 2020), https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm.

For transactions potentially associated with terrorism, banks, along with MSBs, filed approximately 90 percent of suspicious activity reports (SARs) flagged for TF between 2017 and 2020.[89] Banks accounted for approximately a quarter of those SARs, with MSBs responsible for filing the rest. As noted earlier, most of the suspicious transactions identified for suspected TF are outbound transfers made by U.S. persons seeking to provide funds to terrorist groups active outside of the United States. The low value of most person-to-person transactions associated with terrorism (one assessment found most SARs involved suspicious transactions less than $800) and the sheer size and scope of financial flows through the U.S. financial system give terrorist organizations and their financiers the opportunity to blend in with normal financial activity.

As noted in the 2018 NTFRA, the senders and receivers of most terrorist-related transfers seek to conceal the true source and purpose of, and parties involved in, the transactions in order to conceal their activities. For example, sending funds to a jurisdiction in close proximity to an active terrorist group may be one contextual indicator of potential TF transactions. But some terrorist groups have more frequently used intermediaries in third countries to collect funds, which are then commingled with funds from other supporters and transferred to the terrorist organization. The added layer obfuscates the network, making it more difficult to draw connections to TF-related activity.

Since the 2018 NTFRA, one of the changes observed is a shift in person-to-person transfers away from Iraq and Syria and toward other jurisdictions in the Middle East, Africa, and South and Southeast Asia in or near areas where ISIS and AQ operate. This presents a challenge for U.S. banks because it may mean that U.S. persons seeking to provide funds or travel to support these groups look to facilitators acting on behalf of branches or affiliates in these areas.

A second challenge for U.S. banks relates to unknowingly moving funds affiliated with terrorism when they provide correspondent banking services to other foreign financial institutions. When providing these services, a U.S. bank serves as an intermediary, or a respondent bank, without having a direct relationship with the originator or beneficiary of the transactions and relies on the correspondent bank to identify and mitigate risk associated with that customer.[90] For example, ineffective insider threat mitigation practices at a correspondent bank could expose the U.S. bank to complicit employees facilitating TF activity. This can lead to the U.S. bank unwittingly process transactions from foreign banks on behalf of complicit institutions or individuals. These complicit individuals can include local money remitters whose employees or owners may act on behalf of ISIS or others.[91] They can also include larger funds transfers sent on behalf of Hizballah or its financial supporters, or funds routed by Iran to support terrorist proxies, regional militant groups, or other malign activity.[92]

89 FinCEN, *SAR Stats*, https://www.fincen.gov/reports/sar-stats.

90 U.S. banks that maintain correspondent accounts for foreign financial institutions (FFI) are required to establish appropriate, specific, and risk-based due diligence policies, procedures, and processes that are reasonably designed to assess and manage the risks inherent with these relationships. Under existing U.S. regulations, there is no general requirement for U.S. depository institutions to conduct due diligence on an FFI's customer. See *Department of the Treasury and Federal Banking Agencies Joint Fact Sheet on Foreign Correspondent Banking*, p. 2 (Aug. 30, 2016).

91 See, for example, Department of the Treasury, OFAC, "Treasury Targets ISIS Financial Facilitators in Syria and Turkey," (May 17, 2021), https://home.treasury.gov/news/press-releases/jy0179.

92 In March 2021, the Department of Justice announced criminal charges in a nearly 20-year-long scheme to evade U.S. sanctions on Iran. As part of the scheme, the defendants allegedly made false representations to financial institutions to disguise more than $300 million worth of transactions on Iran's behalf, using money wired in U.S. dollars and sent through U.S.-based banks. Department of Justice, "Iranian Nationals Charged with Conspiring to Evade U.S. Sanctions on Iran by Disguising $300 Million in Transactions Over Two Decades," (Mar. 19, 2021), https://www.justice.gov/opa/pr/iranian-nationals-charged-conspiring-evade-us-sanctions-iran-disguising-300-million.

As noted in the 2018 NTFRA, Hizballah presents a particular challenge because of its regular use of the international banking system and its significant financial resources, primarily due to the hundreds of millions of dollars per year provided by Iran. Hizballah is able to access foreign financial institutions through supporters or sympathizers that willingly execute transactions on behalf of Hizballah leaders, facilitators, or affiliated entities. In August 2019, Treasury sanctioned Jammal Trust Bank (JTB), a Lebanon-based financial institution that knowingly facilitated banking activities for Hizballah.[93] JTB was alleged to have a long-standing relationship with a key Hizballah financial entity and to have provided financial services to Hizballah's Executive Council and the Iran-based Martyrs Foundation.[94]

Further, Hizballah is not subject to UN-targeted financial sanctions and is not domestically designated as a terrorist organization by a significant number of foreign jurisdictions. For example, while the United States, UK, Canada, Australia, Germany, and Israel have designated all of Hizballah as a terrorist group, the European Union (EU) has only designated the military wing of Hizballah. This could allow Hizballah political leaders or social welfare groups to open accounts and move funds through EU banks. The limited use and uneven implementation of counterterrorism sanctions by foreign governments and foreign financial institutions remain a challenge, as these designations help cut off the specific facilitators from the international financial system and serve as a useful resource in identifying financial activity associated with other terrorist networks.

For DVE activity, transactions through personal bank accounts or accounts held by online payment services are the most common. Such activity can include sending funds to supporters or websites fundraising on behalf of violent extremist groups, purchasing weapons or other material (such as tactical and survival gear, components for explosives, etc.), or traveling domestically to engage in paramilitary training.[95] For example, four individuals associated with violent white supremacist groups were charged with several criminal acts, including allegedly conspiring to damage the property of an energy facility in the United States and allegedly conspiring to manufacture, transport, and sell hard-to-obtain firearms and firearm parts in a manner that would hide these purchases from the federal government. Two of the individuals allegedly used their personal bank accounts as well as online payment platforms linked to those accounts to transfer funds related to the manufacturing of illegal firearms.

The prominent use of bank accounts and online payment platforms for DVE-linked financial activity may not be related to a particular vulnerability of these products, but rather their dominant role in facilitating person-to-person payments for domestic transactions more generally. However, it has been noted that some DVEs may be more inclined to use regulated financial institutions to move funds compared to other perpetrators of terrorism.[96] Financial transactions by undesignated U.S. persons or groups promoting extremist rhetoric are generally not prohibited and they are not illegal unless associated with a planned violent act or other illicit activity.

An additional challenge for banks is that many transactions associated with terrorism or TF are often hard to distinguish from legitimate day-to-day transactional activity without additional information about the sender or recipient, or other indicia of illicit activity. This makes derogatory information about the subjects of a transaction very relevant to identifying TF activity. One review of financial reporting associated with potential terrorist activity noted that financial institutions frequently flagged suspicious activity due to information received from law enforcement, a subject's connection to a weapon, or a thwarted or completed attack.[97] As previous NTFRAs

93 Department of the Treasury, OFAC, "Treasury Labels Bank Providing Financial Services to Hizballah as Specially Designated Global Terrorist," (Aug. 29, 2019), https://home.treasury.gov/news/press-releases/sm760.

94 Id.

95 Some of this activity may be protected by the U.S. Constitution.

96 FATF REMT Report, pp. 21-22.

97 Treasury analysis of financial institution reporting.

have noted, some suspected terrorists or terrorist financiers may engage in transactional activity that may have other indicia of potentially illicit activity, such as structuring or activity inconsistent with a customer's profile. One assessment of financial reporting found that approximately 30 percent of the relevant reports linked to suspected terrorists identified suspicious deposits in accounts, including suspected cash or check structuring, or suspicious transactions with an unknown source or use of funds.[98]

Money Services Businesses

MSBs play an essential role in providing financial services to those who may have limited access to mainstream banks, and they serve as a vital channel for millions of Americans who send money to family and others around the world. As of 2019, approximately one-quarter of U.S. households used non-bank financial institutions, including money transmitters.[99] In terms of international remittances, U.S. consumers transferred 325 million remittances worth $175 billion in 2017, 95 percent of which went through MSBs.[100] In conflict zones and other areas without a well-developed banking system, MSBs may fulfill critical humanitarian or economic needs and be the only financial lifeline for those who rely on remittances for food and shelter.

Like banks, terrorist financiers have misused MSBs to move money around the world. Between 2017 and 2020, MSBs filed approximately 70 percent of all SARs flagged for TF.[101] An analysis of financial activity associated with U.S.-based individuals charged with supporting terrorist activity found that funds moved via MSBs were most commonly used for travel-related purchase activity or were associated with foreign travel (e.g., using an MSB in a jurisdiction near a conflict zone). MSBs will likely remain a preferred method for moving terrorist-related funds— largely because MSBs move funds quickly and efficiently through the global financial system; they may not require customers to open an account and in some cases do not verify identification for transactions below certain monetary thresholds; and several multinational MSBs have a worldwide footprint and operate in areas near conflict zones that may not be served by banks.

It is important to note that some large multinational money transmitters, consistent with their identified TF risk, have developed sophisticated internal programs and models to identify potential TF, resulting in the filing of highly useful reports that have supported multiple actions to disrupt terrorism and TF activity. They may also have controls in place for areas of higher TF risk, such as limits on the number or size of transactions. At the same time, terrorist operatives, foreign terrorist fighters (FTFs), and financial facilitators moving funds on behalf of terrorist groups usually send low-value transfers, making detection more difficult for those filing SARs and law enforcement, according to our analysis.

Certain terrorist groups, such as al-Shabaab and other AQ affiliates, frequently use money remitters to transfer funds.[102] MSBs have also been a commonly used channel by which FTFs seeking to join ISIS or other terrorist organizations overseas have transferred funds out of the United States and into conflict zones. While foreign-based violent extremists and DVEs are less likely to use brick-and-mortar MSBs, they have gravitated toward online MSBs and other payment platforms and services that facilitate electronic funds transfers.[103]

98 Id.

99 2019 FDIC Household Banking Survey.

100 Consumer Financial Protection Bureau, *Remittance Rule Assessment Report*, p .4, (Apr. 2019), https://files.consumerfinance.gov/f/documents/bcfp_remittance-rule-assessment_report_corrected_2019-03.pdf.

101 FinCEN, *SAR Stats*, https://www.fincen.gov/reports/sar-stats.

102 Al-Shabaab primarily operates in Somalia, which is almost exclusively dependent on money remitters for access to the international financial system.

103 FATF REMT Report, p. 15.

MSBs in the United States are vulnerable to abuse for TF for a number of reasons. First, they may unknowingly move funds on behalf of terrorists and their supporters. In some instances, complicit employees or owners may also willingly facilitate TF in violation of applicable laws, regulations, and the MSB's own AML/CFT policies and procedures. Finally, a challenge similar to banks is that the range in resources available to an individual MSB may lead to inadequate AML/CFT controls. While not necessarily a vulnerability for larger entities, it may be an issue for smaller MSBs that support online person-to-person funds transfers but lack a comprehensive understanding of TF risk. This also highlights the importance of compliance and effective supervision. Additionally, similar to banks, many funds transfers sent through MSBs associated with TF or terrorism do not appear, on their face, to have a link to terrorism, which would be difficult for MSBs to detect without information from law enforcement.

The problem of complicit employees is particularly difficult for MSBs because they often operate via agents, who have a more attenuated relationship with MSBs than a full-time employee might. This risk is pronounced among smaller MSBs or MSBs that offer money services as an ancillary component to their primary business, such as a convenience store that cashes checks or a hotel that provides currency exchange.

U.S.-based MSBs may also face some risk from foreign agents or MSBs with whom they partner. This may be especially true in conflict-affected jurisdictions where access to banking services is limited and terrorist organizations operate. In these areas, remittance providers may be the primary financial institutions through which consumers can conduct cross-border funds transfers. Moreover, the cash-intensive and informal nature of some remittance services can expose such entities to TF risks.[104]

For instance, ISIS has exploited several licensed money remitters and exchange houses in or near areas where it operates to access the international financial system. In some instances, they have been assisted by complicit employees or owners. For example, in September 2019, Treasury designated the Al-Khalidi Exchange for providing financial, material, or technological support for, or goods or services to, ISIS.[105] As of September 2017, all locations were run by two individuals who knowingly assisted ISIS members in financial transfers. As of early 2017, al-Khalidi in al-Raqqah, Syria, and Gaziantep, Turkey, were involved in ISIS's transfer of funds from Iraq through al-Raqqah to Gaziantep in support of ISIS. As of late 2016, Al-Khalidi in Sanliurfa, Turkey, was the most important financial transfer office in the region used to move hundreds of thousands of dollars per day to ISIS-held areas.

Unlicensed Money Transmission

Individuals and entities that provide funds transfers and other financial services in the United States do not always comply with licensing and regulatory requirements. A variety of businesses, including grocery or convenience stores, gas stations, and liquor stores, have been identified as operating as unlicensed money transmitters.[106] In terms of TF activity, these unlicensed money transmitters have been used more frequently to move funds on behalf of AQ and its regional affiliates, such as AQ in the Arabian Peninsula, and al-Shabaab, than other terrorist groups. They may also facilitate transactions for ISIS, its regional affiliates, and non-bank financial institutions, such as exchange houses, that transfer funds on their behalf.

104 See, for example, Department of Justice, "Iranian Nationals Charged with Conspiring to Evade U.S. Sanctions on Iran by Disguising $300 Million in Transactions Over Two Decades," (Mar. 19, 2021), https://www.justice.gov/opa/pr/iranian-nationals-charged-conspiring-evade-us-sanctions-iran-disguising-300-million: "During the scheme, the defendants allegedly created and used more than 70 front companies, money service businesses, and exchange houses – often using the name "Persepolis" or "Rosco" – in the United States, Iran, Canada, the United Arab Emirates, and Hong Kong."

105 Department of the Treasury, OFAC, "Treasury Targets Wide Range of Terrorists and Their Supporters Using Enhanced Counterterrorism Sanctions Authorities," (Sep. 10, 2019), https://home.treasury.gov/news/press-releases/sm772.

106 See FinCEN, FinCEN Advisory, *Informal Value Transfer Systems*, FIN-2010-A011 (Sep. 1, 2010).

For U.S. authorities, the TF risk in this area results from the ongoing challenge of identifying individuals or businesses that act as unlicensed money transmitters, which largely serve populations that cannot or choose not to use legitimate channels. By not complying with applicable AML/CFT requirements, these individuals and entities can facilitate illegal transactions that may support terrorist groups, including ISIS and its regional affiliates, AQ and its regional affiliates, and other foreign terrorist groups.

Cash

Cash is used both domestically and internationally to settle payments and transfer funds in a wide array of transactions, both legitimate and illicit. Some cash transactions are subject to AML/CFT controls, including reporting and record-keeping requirements. However, terrorists and other criminals use cash because it can offer a degree of anonymity, portability, and liquidity, and it can also lack an audit trail. When combined with the significant use of U.S. currency around the world to facilitate day-to-day businesses activities, these features have made cross-border cash transactions, both below and above applicable reporting thresholds, an important means for terrorists and their supporters to move funds from the United States to support operations overseas. As financial institutions (to include banks and money transmitters) have enhanced their AML/CFT controls, operating within the regulated financial system has become more risky, costly, and time-intensive for TF networks. In response, terrorists, as well as other criminal actors, have more frequently turned to cash to transfer funds.

U.S. authorities have identified U.S.-based terrorist financiers supporting a variety of foreign terrorist organizations through the movement of funds in cash, as well as U.S.-based FTFs who travel overseas with cash. For example, in November 2020, an individual was sentenced to 78 months in prison and three years of supervised release after pleading guilty to financing terrorism.[107] Between November 2014 and April 2015, the individual helped her husband and brother-in-law join ISIS by making multiple trips to Hong Kong and transporting more than $30,000 in cash and gold from the United States and depositing it in a safe deposit box in Hong Kong.[108] The individual melted down the gold to look like jewelry and did not disclose the cash and gold on customs declaration forms.[109] When the individual transported the money and gold, she knew that the two men had expressed an interest in joining ISIS and that they intended to use these resources to support ISIS.[110]

Some FTFs and terrorist financiers have used cash for transactions specifically because of its anonymity. On June 14, 2014, Turkish authorities arrested an individual for illegally crossing into Syria from Turkey. During an interview by an FBI agent in 2018, the individual allegedly admitted that he purchased an airline ticket to Gaziantep, Turkey, with cash to avoid creating an electronic record of the purchase. The individual was indicted in February 2021 for attempting to provide material support to ISIS.

Along with these smaller terrorist networks and facilitators, Iran has also sought U.S. currency for its regional proxies or to otherwise support malign activities around the world. For example, on May 10, 2018, Treasury designated a currency exchange network that had procured and transferred millions of dollars of U.S. banknotes into and out of Iran to be used by the Islamic Revolutionary Guard Corps (IRGC)-Qods Force, which supports Iran's malign activities and facilitates Iranian support to regional proxy groups.[111]

---

107 Department of Justice, "Former Elkhart, Indiana Resident Sentenced to Over Six Years in Prison for Financing of Terrorism," (Nov. 9, 2020), https://www.justice.gov/opa/pr/former-elkhart-indiana-resident-sentenced-over-six-years-prison-financing-terrorism.

108 Id.

109 Id.

110 Id.

111 Department of the Treasury, OFAC, "United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF," (May 10, 2018), https://home.treasury.gov/news/press-releases/sm0383.

There have also been instances of DVEs using cash to purchase weapons, tactical gear, or other material to support planned attacks or paramilitary training being conducted in preparation for a violent act. While most of these individuals continue to use credit or debit cards or other electronic payment methods for purchases, some DVE networks believe that using cash allows for increased anonymity and reduces the chance of drawing law enforcement scrutiny.

It is difficult—if not impossible—to completely stop the use of cash smuggling. The anonymity and portability of cash, combined with the widespread demand for U.S. currency globally, means that terrorist groups will continue to use cash smuggling as an alternative for moving funds globally.

Virtual Assets

In the United States, digital assets[112] is a broad term that includes so-called digital currencies, stablecoins,[113] and other terms used in the industry. Digital assets can be securities, commodities, derivatives or something else. Public information on investigations often uses the terms *virtual currency* or *cryptocurrency*. 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.[114] Virtual assets, as used in this report, non-sovereign-administered digital assets (such as convertible virtual currencies, like bitcoin and stablecoins) but do not cover central bank-issued digital currencies (CBDCs), which are representations of fiat currency and treated the same as fiat currency by the FATF. [115]

Some virtual assets allow near instantaneous transactions without the involvement of a financial institution with AML/CFT obligations. These transactions may also be transferred across jurisdictional boundaries and are pseudonymous.[116] VASPs doing business in whole or part in the United States qualify as money transmitters, which means they are required to comply with AML obligations that apply to MSBs, including registering with FinCEN; developing, implementing, and maintaining an effective risk-based AML program; filing SARs and currency transaction reports; and maintaining certain records. When VASP operators neglect their AML obligations, such as failing to establish an effective AML program or report suspicious activities, their actions create vulnerabilities for the financial system (and violate AML regulations). Some virtual assets may fall under the jurisdiction of the SEC, the CFTC, or other authorities, and service providers of these assets could be subject to AML obligations.

Virtual assets, along with other emerging financial technologies, can provide potential benefits for consumers and reduce the speed and cost of financial services. These same products and technologies may also be vulnerable to abuse by terrorist financiers because they can enable anonymous cross-border peer-to-peer funds transfers, which

112 FinCEN, CFTC, and SEC, *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets*, (Oct, 11, 2019), https://www.fincen.gov/sites/default/files/2019-10/CVC%20Joint%20Policy%20Statement_508%20FINAL_0.pdf.

113 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 and 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, FDIC, and OCC, Report on Stablecoins (Nov. 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

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

115 CBDCs may have unique money laundering and terrorist financing 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 it consideration data privacy and other concerns.

116 Lexis-Nexis, White Paper, *A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Dec. 2019), https://risk.lexisnexis.com/global/en/insights-resources/white-paper/a-risk-based-approach-to-virtual-assets.

can occur without the involvement of a VASP with AML obligations.[117]

While such cases are still less prevalent than those involving traditional financial assets, U.S. authorities have identified several instances where terrorist groups and their financial supporters solicited funds in virtual assets, usually through a social media platform or other internet-based crowdsource platform. This has included supporters of several international terrorist groups, as well as some DVE groups. In August 2020, U.S. law enforcement announced the dismantling of several TF cyber-enabled campaigns involving the al-Qassam Brigades, HAMAS's military wing, ISIS, and AQ, as detailed in several criminal complaints.[118] Two of these campaigns—as discussed in more detail below—included the solicitation of virtual asset donations from around the world. Each group used virtual assets and social media to garner attention and raise funds for their terror campaigns.

- One cyber-enabled TF campaign involved an alleged scheme by AQ and affiliated terrorist groups, largely based out of Syria (as also discussed in the AQ section).[119] As the forfeiture complaint alleges, these terrorist organizations operated a bitcoin ML network using Telegram channels and other social media platforms to solicit virtual asset donations to further their terrorist goals. As alleged in some instances, they purported to act as charities when, in fact, they were openly and explicitly soliciting funds for violent terrorist attacks.
- Another campaign involved the al-Qassam Brigades and its online virtual asset fundraising efforts. In the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps. The al-Qassam Brigades boasted that bitcoin donations were untraceable and would be used for violent causes. While the group initially requested that virtual assets be sent to a single virtual asset address hosted at a U.S.-based exchange, they subsequently developed and relied on technology that generated a new unique virtual asset address for each transaction to make the transactions harder to trace.[120] Their websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor. The evolution indicates terrorist groups can adapt to risk-mitigation efforts and exploit nuanced vulnerabilities within this emerging technology.

Foreign-based RMVE groups and some DVEs have also sought to solicit or transfer funds in virtual assets or expressed interest in using virtual assets to move funds pseudonymously or in bolstering anonymity through anonymity-enhancing technologies. Brenton Tarrant, who attacked a Christchurch, New Zealand, mosque in March 2019, transferred funds using virtual assets to ideologically aligned groups and individuals in Europe.[121] For some groups, the use of virtual assets represents an opportunity to enhance their anonymity compared to other financial services. For others it is an alternative to online payment platforms that will no longer permit them to use their services. Additionally, some of these groups make extensive use of social media and encrypted applications to reach potential supporters and rely largely on online solicitations. However, while terrorist use of virtual assets has become more prominent since the 2018 NTFRA, according to information available to the U.S. government, the vast majority of terrorist funds raised in the United States still move through banks and money transmitters or are in cash. As virtual asset penetration in the overall economy increases, the usage by terrorists is also likely to increase.

117 Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, p. 16, (Oct. 2021), www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html; see also remarks by Deputy Secretary of the Treasury Wally Adeyemo at LINKS Conference Presented by Chainalysis (Nov. 4, 2021), https://home.treasury.gov/news/press-releases/jy0466.

118 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," (Aug. 13, 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

119 Id.

120 *U.S. v. Facemaskcenter.com and Four Facebook Pages* (Indictment) (E.D. Mo., Aug. 5, 2020).

121 FATF REMT Report, p. 25.

Additionally, U.S. authorities have identified instances of terrorist groups using or attempting to use virtual assets to pay for certain goods or services, although the vast majority of observed terrorist activity linked to virtual assets involves the solicitation of funds. While bitcoin has been the primary virtual asset solicited by terrorist groups, some groups or individuals are also seeking to use other virtual assets they believe may provide additional anonymity. Some terrorists that use virtual assets have recognized that transactions on public blockchains can be traced and that analytics may be used in some cases to identify parties to a transaction. Bitcoin is likely preferred at present simply because it is more prevalent overall and offers greater liquidity.

While these cases indicate that some terrorists, terrorist groups, and their supporters have used or are seeking to use virtual assets for transactional activity, terrorist use of virtual assets appears to remain limited when compared to other financial products and services. As some terrorist groups operate in jurisdictions with limited financial and telecommunications infrastructure, it can be difficult to convert virtual assets to a fiat currency. Exchanging virtual assets for cash is often necessary for the funds to have utility for a terrorist group as most merchants and businesses, and many financial institutions, do not accept virtual assets as a means of payment, although their use among merchants is growing. Apart from stablecoins, the volatility of their value can also reduce their usefulness to terrorists as a medium of exchange.

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 more widely accepted to pay for goods and services, they may become more popular among terrorist groups. An additional challenge is the extent to which countries subject VASPs to effective AML/CFT regulation and supervision. Many VASPs operating abroad have substantially deficient AML/CFT programs, particularly in jurisdictions where international standards for VASPs are not effectively implemented. 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. While regulatory arbitrage is a problem with all financial services, it is in particular a concern with VASPs given the ability to transfer virtual assets across borders nearly instantaneously, potentially exposing the U.S. financial system to VASPs with deficient or nonexistent AML/CFT controls operating abroad. Domestically, one potential vulnerability may be the growing number of virtual asset kiosks that allow individuals to quickly convert virtual assets into fiat, especially if these entities do not implement effective AML/CFT measures.

Misuse of Charitable Organizations

As the U.S. government has noted repeatedly, U.S.-based tax-exempt charitable organizations, whether through their work in the United States or internationally, play a vital role in providing aid to vulnerable populations and those in need of emergency assistance.[122] This has become particularly important during the COVID-19 pandemic, during which these organizations have provided medical, food, housing, employment, and counseling services to tens of millions of Americans directly affected by the pandemic. Outside of the United States, these organizations help empower women and girls with health and education services, rebuild communities shattered by violence and conflict, and support political reconciliation, transparency, and accountability in developing countries, among other items. They can also play an important role in countering terrorism, including through their work in

122 See, for example, The White House, *National Security Memorandum on United States Global Leadership to Strengthen the International COVID-19 Response and to Advance Global Health Security and Biological Preparedness*, (Jan. 21, 2021); *Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations*, (Nov. 19, 2020); Department of the Treasury, OFAC, "Treasury Underscores Commitment to Global Flow of Humanitarian Aid in Face of COVID-19 Pandemic," (Apr. 9, 2020), https://home.treasury.gov/news/press-releases/sm969.

preventing radicalization to violence and violent extremism.

However, in some instances, terrorist groups have misused these organizations to support their activities. This has included instances where donations to a charitable organization were intentionally routed to terrorist groups and where a charitable organization knowingly or intentionally provided logistical services, recruitment, or otherwise facilitated support to a terrorist group in a conflict zone. It should be noted that these events remain infrequent compared to the overall population of charitable organizations in the United States.

Additionally, risk occurs when terrorist supporters set up sham charities that do not actually provide any charitable services but serve as a cover for raising funds for a foreign terrorist group. For example, while not a U.S.-based charitable organization, the Nejaat Social Welfare Organization (Nejaat), which was designated by Treasury, is illustrative of how U.S.-based organizations could be abused.[123] Nejaat was used as a cover company to facilitate the transfer of funds to and support the activities of ISIS-Khorasan (ISIS-K). In late 2016, Afghan leaders of ISIS-K held planning meetings under the cover of a Salafi solidarity meeting sponsored by Nejaat. Executive members of Nejaat and prominent Salafi leaders in Afghanistan led the meeting, some of whom were financial supporters of Nejaat. Rohullah Wakil, who was also designated by Treasury, was one of the executive members of Nejaat who co-led the meeting. An ISIS-K recruiter, who worked at Nejaat, recruited ISIS-K fighters in Kabul, Afghanistan, and arranged for their travel to Nangarhar Province. Nejaat also collected donations on behalf of ISIS-K from individuals in Qatar, the UAE, Iraq, and other Middle Eastern countries. Money was then transferred from countries in the Persian Gulf to Asia—via the banking system—where an ISIS-K coordinator collected the transferred funds. Nejaat's offices in Kabul and Jalalabad, Afghanistan, distributed the funds to ISIS-K commanders.

Moreover, U.S. authorities have identified other instances where terrorist supporters engaged in fraudulent fundraising under the auspices of a charitable cause but without the participation of any charitable organization. For example, according to allegations in an indictment, an individual involved with a group of women from more than a dozen countries around the world ran a fundraising ring to provide financial support to al-Shabaab from February 2011 through July 2014.[124] The individual was allegedly involved in fundraising in the Netherlands under false pretenses by representing to donors that money was collected to fund charitable ventures, such as schools for orphans, when it was in fact being funneled to terrorists. Additionally, ISIS members and their families residing in Syria's al-Hawl Refugee Camp have used charitable appeals to receive funds from foreign supporters.[125]

Although some charities and NPOs have been misused to facilitate terrorist financing, Treasury and other U.S. government agencies note that most charities and NPOs fully comply with the law, that not all tax-exempt charitable organizations present the same level of TF risk, and that the vast majority of U.S.-based tax-exempt charitable organizations face little or no risk of being abused for TF. However, some organizations, based on their activities and geographic profile, may be more vulnerable to TF abuse. As noted in earlier NTFRAs, those U.S.-

123 Department of the Treasury, OFAC, "Treasury Designates ISIS Financial, Procurement, and Recruitment Networks in the Middle East and South Asia," (Nov. 18, 2019), https://home.treasury.gov/news/press-releases/sm831.

124 Department of Justice, "Dutch National Faces Charges for Participation in Terror Financing Ring," (Oct. 29, 2021), https://www.justice.gov/opa/pr/dutch-national-faces-charges-participation-terror-financing-ring. Two U.S.-based members of the fundraising ring were convicted in 2016 for their participation and were sentenced to 12- and 11-years imprisonment, respectively. See also Department of Justice, "Manchester Man Guilty of Lying to Federal Law Enforcement During Interview," (Sep. 19, 2019), https://www.justice.gov/usao-ct/pr/manchester-man-guilty-lying-federal-law-enforcement-during-interview.

125 *The Wall Street Journal*, Refugee Camp for Families of Islamic State Fighters Nourishes Insurgency, (Jun. 9, 2021), https://www.wsj.com/articles/refugee-camp-for-families-of-islamic-state-fighters-nourishes-insurgency-11623254778; see also *The Guardian*, How Women of ISIS in Syrian Camps are Marrying Their Way to Freedom, (Jul. 2, 2021), https://www.theguardian.com/world/2021/jul/02/women-isis-syrian-camps-marrying-way-to-freedom; https://www.lawfareblog.com/crowdfunding-women-islamic-state.

based organizations operating in conflict zones where terrorist groups are active may face risk that their local activities, including social services or financial support, will benefit terrorist groups. This could include in-country staff, partners, or contractors who are knowingly or intentionally but clandestinely providing funds or material from the organization to terrorist supporters.

At the same time, the U.S. government acknowledges that many of the reputable, legitimate organizations involved in this work implement a range of risk-mitigation measures, including due diligence, governance, transparency, accountability, and other compliance measures, even in crisis situations.[126] Since the publication of the 2018 NTFRA, these organizations have sought to enhance and adapt these measures in response to changing risks and their activities in areas where terrorist groups operate. Additionally, organizations that receive funding from the U.S. Agency for International Development (USAID) and are active in high-risk environments are subject to additional vetting measures by USAID and must implement due diligence and risk-mitigation requirements to ensure full compliance of U.S. sanctions, including threats posed by terrorist organizations.[127]

The U.S. government also notes that U.S. charitable organizations have reported increasing financial access challenges when dealing with high-risk jurisdictions.[128] These financial access challenges have led to some organizations resorting to other ways to transfer funds, including physically moving cash, which can introduce other risks, including for terrorist financing abuse.[129] As such, the U.S. government has and will continue to encourage the implementation of proportionate and risk-based AML/CFT measures to ensure legitimate humanitarian assistance flows to those most in need.[130]

126 Department of the Treasury, OFAC, "Treasury Underscores Commitment to Global Flow of Humanitarian Aid in Face of COVID-19 Pandemic" (Apr. 9, 2020), https://home.treasury.gov/news/press-releases/sm969.

127 See U.S. Agency for International Development, *Partner Vetting*, https://www.usaid.gov/work-usaid/partner-vetting-system#:~:text=Partner%20vetting%20is%20an%20enhanced,terrorists%2C%20or%20affiliates%20of%20terrorists; see also U.S. Agency for International Development, "ANNEX 1- RISK ASSESSMENT AND MANAGEMENT PLAN FOR HIGH RISK ENVIRONMENTS" (Jan. 2022), https://www.usaid.gov/sites/default/files/documents/ANNEX_1Risk_Assessment_and_Management_Plan_for_High-Risk_Environments.pdf.

128 See, for example, Department of the Treasury, "READOUT: Deputy Secretary of the Treasury Wally Adeyemo's Meeting with Nongovernmental Organizations Operating in Afghanistan" (Dec. 22, 2021), https://home.treasury.gov/news/press-releases/jy0547.

129 See Financial Action Task Force, *High-Level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards*, p. 2, (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/Unintended-Consequences.pdf.

130 Department of the Treasury, FinCEN, "FinCEN and Federal Banking Agencies Clarify BSA Due Diligence Expectations for Charities and Non-Profit Customers," (Nov. 19, 2020), https://home.treasury.gov/news/press-releases/sm1183.

CONCLUSION

Two decades after the U.S. response to AQ in Afghanistan following the 9/11 attacks, terrorists and their methods of financing have evolved into a multifaceted and globally dispersed threat that encourages followers to finance their own attacks.[131] Globally, these groups and networks have sought to use online connectivity to recruit and inspire like-minded individuals who can engage in violence while reducing their operational footprint and potential vulnerability to disruption. Along DVEs who rely on similar self-financing methods, they are the most urgent terrorism threat to U.S. national security. As the number of DVE movements and ideologies continue to grow, identifying and understanding the associated TF risk is increasingly important.

Keeping our citizens safe and our financial system from becoming an enabler of these violent attacks continues to require a continued whole-of-government approach, to include effective coordination between and among Treasury, law enforcement, and the private sector, as well as with our foreign partners. This includes regularly updating our understanding of TF risk and staying ahead of technological changes and shifts in payments and transactions that create new vulnerabilities that terrorists may exploit. While new security challenges, such as the emergence of renewed great power competition and the threat of another global pandemic, will become an ever-increasing focus of the U.S. national security community, we must not let up pressure and maintain our leadership role in combating TF.

131 See ODNI 2021 Threat Assessment, p. 23; see also Testimony of FBI Director Christopher Wray, *Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11*, (Sep. 21, 2021).

List of Acronyms

ACH	Automated Clearinghouse
AEC	Anonymity-Enhanced Cryptocurrencies
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
ANF	Al-Nusrah Front
AQ	al-Qa'ida
BSA	Bank Secrecy Act
BSA/AML	Bank Secrecy Act / Anti-Money Laundering
CBDC	Central Bank-Issued Digital Currencies
CBP	U.S. Customs and Border Protection (Department of Homeland Security)
CDD	Customer Due Diligence
CFTC	Commodity Futures Trading Commission
CIP	Customer Identification Program
CPF	Countering Proliferation Financing
CTR	Currency Transaction Report
CVCs	Convertible Virtual Currencies
DeFi	Decentralized Finance
DHS	Department of Homeland Security
DOJ	Department of Justice
DPA	Deferred Prosecution Agreement
DVE	Domestic Violent Extremists
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FBAs	Federal Banking Agencies
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network (U.S. Department of the Treasury)
FRB	Board of Governors of the Federal Reserve System (or "Federal Reserve Board")
FTF	Foreign Terrorist Fighters
IC	Intelligence Community

ICE HSI	U.S. Immigration and Customs Enforcement Homeland Security Investigations (U.S. Department of Homeland Security)
IEEPA	International Emergency Economic Powers Act
IP	Internet Protocol
IRGC	Islamic Revolutionary Guard Corps
IRS-CI	Internal Revenue Service-Criminal Investigation
ISIS-K	ISIS-Khorasan
IT	Information Technology
JTB	Jammal Trust Bank
LeT	Lashkar-e-Tayyiba
ML/TF	Money Laundering/Terrorist Financing
MSB	Money Services Business
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OCDETF	Organized Crime Drug Enforcement Task Forces (U.S. Department of Justice)
OFAC	Office of Foreign Assets Control (U.S. Department of the Treasury)
OIA	Office of Intelligence and Analysis (U.S. Department of the Treasury)
PPE	Personal Protective Equipment
P2P	Peer-To-Peer
RMVE	Racially or Ethnically Motivated Violent Extremist
SAR	Suspicious Activity Report
SB/SE	Small Business/Self-Employed
SEC	Securities and Exchange Commission
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFI	Terrorism and Financial Intelligence (U.S. Department of the Treasury)
TFFC	Terrorist Financing and Financial Crimes (U.S. Department of the Treasury)
UAE	United Arab Emirates
UAVs	Unmanned Aerial Vehicles
UNSCR	UN Security Council Resolution
VASP	Virtual Asset Service Provider


THE DEPARTMENT OF THE TREASURY
1789