NATIONAL TERRORIST FINANCING RISK ASSESSMENT

2018

National Terrorist Financing Risk Assessment

2018

EXECUTIVE SUMMARY

The 2018 *National Terrorist Financing Risk Assessment* (2018 NTFRA) identifies the terrorist financing (TF) threats, vulnerabilities, and risks that the United States currently faces, updating the 2015 *National Terrorist Financing Risk Assessment* (2015 NTFRA). Relevant component agencies, bureaus, and offices of Treasury, the Department of Justice (DOJ), the Department of Homeland Security (DHS), as well as federal financial regulators and other government agencies participated in the development of the risk assessment. The 2018 NTFRA is based on discussions with relevant authorities and private sector entities, a review of government actions and analysis, and private sector research, issued since the 2015 NTFRA.

The most common type of TF activity in the United States involves individuals who knowingly provide funds to terrorists, terrorist groups, or their supporters abroad. This includes multiple groups designated by the United States as foreign terrorist organizations (FTOs), including the Islamic State of Iraq and Syria (ISIS) and its regional affiliates, Al-Qaida (AQ) and its regional affiliates, Al-Nusrah Front (ANF), Al-Shabaab, Hizballah, and Hamas.[1] These groups and their supporters target individuals sympathetic to humanitarian causes or vulnerable to violent messaging and aggressively use social media to identify potential followers, recruit, and solicit financial or other forms of material support.

ISIS-related financial activity in the United States is most commonly associated with U.S. persons traveling or aspiring to travel abroad to join ISIS in Iraq or Syria or other jurisdictions where ISIS regional affiliates are active, although the number of U.S. persons traveling or attempting to travel to Syria and Iraq has declined since 2015. Funds used to support travel-related activity have primarily been generated from legitimate activities. In some instances U.S.-based individuals have raised or solicited funds specifically for ISIS. ISIS financiers and supporters abroad also send funds to other ISIS supporters or regional affiliates in foreign jurisdictions that may be routed through the U.S. financial system, and may seek to procure sensitive or controlled goods from U.S.-based companies.

Other terrorist groups besides ISIS are also active financially in the United States. Hizballah members and supporters and individuals supporting other terrorist groups, as well as foreign terrorist fighters (FTFs), continue to raise funds from small-scale criminal activity, such as bank or credit card fraud, as well as from legitimate commercial activity. Hizballah-affiliated networks also continue to seek to procure sensitive or controlled goods from the United States. AQ and its regional affiliates, as well as associated groups such as ANF, continue to seek funds and other resources from U.S.-based supporters. Hizballah-affiliated networks continue to generate revenue from drug trafficking or organized criminal activity that has a U.S. nexus. Al-Shabaab continues to work through U.S.-based facilitators to raise funds from witting supporters as well as seeking funds from unwitting donors under the false pretenses of charity but outside of any tax-exempt charitable organization. Other terrorist groups, such as Hamas, also continue to look to the United States as a venue for revenue generation.

[1] Several regional affiliates of ISIS and AQ have been separately designated as FTOs, including ISIS Sinai Province, ISIS-Libya, ISIS-Khorasan, ISIS-Philippines, ISIS-Bangladesh, ISIS- West Africa, Al-Qaida in the Arabian Peninsula (AQAP), and AQ in the Indian Subcontinent.

U.S.-based terrorist supporters seek to place their often legitimately-earned funds into the financial system and transfer the funds abroad. Due to prevalence and accessibility, banks and money services businesses (MSBs) are the most commonly used channels. Due to the centrality of the U.S. financial system and the U.S. dollar, U.S. banks continue to face TF risk from their role in U.S. dollar clearing and processing international payments. Importantly, due to the nature of terrorist financing (often legitimately-sourced funds later used to fund illicit activity), U.S. banks face challenges in distinguishing terrorism-related financial transactions from licit activity.

Some U.S.-based MSBs face TF risk from the acts of complicit employees, as well as isolated compliance deficiencies among smaller online payment providers that provide person-to-person funds transfers. Unlicensed money transmitters also remain an important channel for some terrorist groups and their supporters. Robust implementation of anti-money laundering/countering the financing of terrorism (AML/CFT) standards by U.S. financial institutions makes cash a secure if inefficient alternative for terrorist groups or supporters that prioritize operational security over the speedy movement of funds.

U.S. tax-exempt charitable organizations that only operate domestically face a low risk of TF abuse. However, there continues to be greater TF risk for the small number of U.S. tax-exempt charitable organizations that operate in high risk regions where ISIS and its regional affiliates, AQ and its regional affiliates, Al-Shabaab, and other terrorist groups are most active, such as Afghanistan, Pakistan, Somalia, Syria, and Yemen.

While there have been isolated instances of terrorist groups and their supporters soliciting funds in virtual currencies, such as bitcoin, and using virtual currencies to move funds or purchase goods or services, virtual currencies do not currently present a significant TF risk, but bears close monitoring as it is only likely to grow. However, lack of regulation and supervision in most jurisdictions worldwide exacerbates the illicit finance and sanctions evasion risks that virtual currency payments present.

As detailed in the *2018 National Strategy for Combating Terrorist and Other Illicit Financing*, the U.S. government employs a comprehensive interagency approach to counter terrorist financing. This includes using law enforcement, financial sanctions, and other financial measures to dismantle and disrupt terrorist financing networks, closing existing gaps in the U.S. financial system that have been used to facilitate TF, and engage with foreign partners and the private sector to develop a secure global framework that will effectively deny terrorist groups the ability to access the international financial system to raise, move and use funds.

INTRODUCTION

The 2018 NTFRA identifies the TF threats, vulnerabilities, and risks that the United States currently faces, updating the 2015 NTFRA.[2] This report together with the 2018 National Money Laundering Risk Assessment (NMLRA) and National Proliferation Financing Risk Assessment (NPFRA) provide an overview of the current illicit finance risks to the United States

TF activity remains a significant concern for the United States because all terrorist groups require financial supporters, facilitators, and networks to keep funds flowing and to accomplish their destructive goals. The United States is particularly vulnerable to TF and other forms of illicit finance because much of the global economy touches the United States and U.S. financial system. The United States is the primary trading partner to dozens of other countries. Even when a U.S. person is not a party to a transaction, the value of the trade is often denominated in U.S. dollars and completed with a U.S. dollar-denominated funds transfer. In addition, physical U.S. currency is used globally as either the primary or de facto secondary functional currency or store of value.

The terminology and methodology of the 2018 NTFRA are based on the guidance of the Financial Action Task Force (FATF), the international standard-setting body for AML/CFT safeguards. The underlying concepts for the risk assessment are *threats* (the terrorist groups most active in raising or moving funds through the United States or U.S. financial system), *vulnerabilities* (the opportunities that facilitate TF), *consequence* (the impact of a vulnerability), and *risk* (the synthesis of threat, vulnerability and consequence).

PARTICIPANTS

This report incorporates published and unpublished research and analysis as well as the insights and observations of the managers and field staff of the following U.S. government agencies that reviewed the report:

- Department of the Treasury
    - Office of Terrorism and Financing Intelligence
        - Office of Terrorist Financing and Financial Crimes (TFFC)
        - Office of Foreign Assets Control (OFAC)
        - Office of Intelligence and Analysis (OIA)
        - Financial Crimes Enforcement Network (FinCEN)
    - Internal Revenue Service
        - Criminal Investigation (CI)
        - Tax Exempt & Government Entities Division (TEGE)
- Department of Justice
    - National Security Division (NSD)
    - Criminal Division
    - Tax Division

[2]The 2015 NTFRA is available at http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

    - Drug Enforcement Administration (DEA)
    - Federal Bureau of Investigation-Terrorist Financing Operations Section (FBI-TFOS)
- Department of Homeland Security
    - Homeland Security Investigations (HSI)
    - Office of Intelligence and Analysis
    - Office of Policy
- Department of State
    - Bureau of Counterterrorism and Countering Violent Extremism
    - Bureau of Economic and Business Affairs
- National Counterterrorism Center (NCTC)
- Staff of the Federal functional regulators[3]

METHODOLOGY

As in the 2018 NPFRA and the updated 2018 NMLRA, the terminology and methodology of the 2018 NTFRA are based on the guidance of the FATF, which presents a process for conducting a risk assessment at the national level. This approach uses the following key concepts:

- **Threat**: A threat is a person, group of people, or activity with the potential to cause harm to, for example, the state, society, the economy, etc.[4] In the TF context this includes terrorist groups and their facilitators, as well as radicalized individuals, seeking to exploit the United States and U.S financial system to raise, move, and use funds.
- **Vulnerability**: A vulnerability is something that can be exploited to facilitate terrorist financing, both in the raising of funds for terrorist networks and the moving 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 in which it may be difficult to distinguish legal from illegal activity.
- **Consequence**: Not all TF methods have equal consequences. The methods that allow for the greatest amount of money to be raised or moved most effectively present the greatest potential TF consequences.[5]
- **Risk**: Risk is a function of threat, vulnerability, and consequence.

Throughout the 2018 NTFRA, potential TF threats, vulnerabilities and risks are identified, analyzed and evaluated in the following manner:

---

[3] This includes staff of: the Commodity Futures Trading Commission (CFTC); the Board of Governors of the Federal Reserve System (FRB); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); the Office of the Comptroller of the Currency (OCC); and the Securities and Exchange Commission (SEC).

[4] FATF Guidance, National Money Laundering and Terrorist Financing Risk Assessment at 7, February 2013.

[5] Given the challenges in determining or estimating the consequences of TF, countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. FATF Guidance, National Money Laundering and Terrorist Financing Risk Assessment at 8, February 2013. Therefore, the 2018 NTFRA focuses on threats and vulnerabilities in determining TF risks. The financing of terrorist acts and of terrorists and terrorist organizations is typically described as a three stage process requiring the raising, movement and use of funds.

- Identifying, through a review of criminal prosecutions, OFAC designations, and financial institution reporting (1) the terrorist groups that are most active in raising and moving funds through the United States and U.S. financial system and (2) the methods and typologies used by those groups to raise and move funds;
- Comparing the above information with intelligence reporting to validate or refute the information;
- Analyzing how the particular characteristics or circumstances of financial products, services, or other entities facilitate the raising or movement of funds on behalf of terrorists or terrorist organizations;
- Assessing the extent to which domestic laws and regulations, law enforcement investigations and prosecutions, regulatory supervision, and enforcement activity and international outreach and coordination mitigate identified TF threats and vulnerabilities; and
- Using the aforementioned research and analysis to identify TF risks facing the United States.

SECTION I. THREATS

A. ISIS

The U.S. and its allies have made significant progress in countering the terrorism and TF threat posed by ISIS. According to U.S. counterterrorism authorities, ISIS has lost over 97 percent of the territory it once controlled in both Iraq and Syria; the number of ISIS fighters in those countries is significantly down, and its illicit income streams are down.[6] Despite this success, U.S. authorities assess ISIS and its regional affiliates pose a continuing terrorist threat to the United States and its allies because of its ideological appeal, media presence, , its global enterprise of almost two dozen affiliates and networks, and proven ability to direct and inspire attacks.[7] Moving forward, the U.S. intelligence community assesses that ISIS is likely to focus on regrouping in Iraq and Syria, enhancing its global presence, championing its cause, planning international attacks, and encouraging its members and sympathizers to attack in their home countries.[8]

While ISIS' ability to generate revenue has been significantly impacted by the loss of territory in Syria and Iraq, the group in continues to derive the vast majority of its revenue from two primary sources of funding, (i) the extortion and taxation of civilian populations and economies in Iraq and Syria, and (ii) the smuggling and sale of oil and oil products. Further, successful efforts to disrupt these and other sources of revenue have forced it to look elsewhere for new funds, including from U.S. persons. These funds have been brought over by U.S. person-FTFs[9] (largely to fund their travel and living expenses) and sent from U.S. persons to ISIS members or supporters in areas bordering territory that ISIS controls or is present in. This activity continues to pose a TF threat despite the reduction in the number of U.S. persons traveling or attempting to travel to Syria and Iraq since 2015. U.S. counterterrorism authorities assess that while some FTF's will depart Syria and Iraq, it is unlikely there will be a mass exodus of FTFs, as many battle-hardened fighters will stay and fight.[10] U.S. law enforcement authorities continue to identify U.S.-based individuals who seek to join the ranks of FTFs traveling in support of ISIS.[11]

The most common ISIS-related financial activity in the United States involves travel-related spending by U.S.-based aspiring FTFs, such as purchasing airplane tickets or other material in anticipation of joining ISIS in Syria, Iraq, or other jurisdictions where its regional affiliates are active. For example, on August 31, 2017, the United States charged an individual with providing

---

[6] Nicholas Rasmussen, Director, National Counterterrorism Center, "CNAS Keynote Policy Address, May 3, 2017. Available at https://www.dni.gov/files/NCTC/documents/news_documents/CNASopeningremarks.pdf.

[7] Christopher Wray, Director, FBI, Testimony before the Senate Committee on Homeland Security and Governmental Affairs, "Current Threats to the Homeland," Sept. 27, 2017. Available at https://www.fbi.gov/news/testimony/current-threats-to-the-homeland.

[8] Daniel Coats, Director of National Intelligence, "Worldwide Threat Assessment of the United States Intelligence Community," Feb. 13, 2018 ("Worldwide Threat Assessment"). Available at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[9] According to the Department of Homeland Security, as of August 2017, approximately 290 U.S. persons have traveled or attempted to travel to Syria and Iraq potentially to fight or otherwise support the conflict. DHS, Reference Aid: US Foreign Fighters. Available at https://www.dhs.gov/sites/default/files/publications/Foreign%20Fighters_CVE%20Task%20Force_Final.pdf.

[10] Nicholas Rasmussen, Director, National Counterterrorism Center, "CNAS Keynote Policy Address, May 3, 2017.

[11] Christopher Wray, Director, Federal Bureau of Investigation, Testimony before the House Committee on Homeland Security, "Worldwide Threats: Keeping America Secure in the New Age of Terror," Sept. 27, 2017.

material support to ISIS and ANF.[12] The individual, along with others, allegedly provided financial support for several U.S.-based FTFs who traveled abroad.[13] This included transfers to the bank account of an individual who used the funds to pay for the travel of another U.S.-based FTF.[14] The United States charged two others in April 2015 with material support to a designated FTO for allegedly collecting more than $1,600 in cash from a number of people in order to provide financial support to an individual attempting to travel to Syria to join ISIS.[15]

While funds from U.S.-based individuals sent to support ISIS appear to be most commonly generated from legitimate activity or personal savings, ISIS supporters in the United States have also engaged in separate criminal activity, such as fraud, to raise money. On November 15, 2016, three individuals were convicted of conspiring to commit murder in Syria on behalf of ISIS and to provide material support to ISIS.[16] One of the individuals was also convicted of one count of attempted financial aid fraud.[17] The individual withdrew more than $1,000 in federal financial aid funds to purchase airplane tickets from the U.S. to destinations in Europe, with the ultimate goal of joining ISIS in Syria.[18]

Some U.S. persons also raise or solicit funds specifically for ISIS, although in many cases these individuals have also provided other types of material support to ISIS. For example, in February 2015, U.S. authorities arrested six individuals who allegedly collected thousands of dollars via bank and non-bank wires from ISIS sympathizers in the United States.[19] According to prosecutors, the group wired the money via an MSB to an ISIS supporter abroad who then transferred the funds in cash to a U.S. person fighting in Syria.[20] Prosecutors allege the money was used to buy clothes and other equipment for ISIS fighters in Syria.[21] In another case, an individual charged in July 2016 allegedly sent funds via an electronic transfer service to a person he believed was collecting money for ISIS to purchase weapons and ammunition for ISIS fighters.[22] The individual also allegedly posted content on social media indicating his support for ISIS and for attacks targeting police officers, military personnel and civilians.[23] In another case, an individual pleaded guilty to attempting to provide material support to ISIS in July 2017.

---

[12] DOJ, Press Release, "Defendant Charged With Conspiring and Attempting to Provide Material Support to ISIS and Al-Nusrah Front," Aug. 31, 2017. Available at https://www.justice.gov/opa/pr/defendant-charged-conspiring-and-attempting-provide-material-support-isis-and-al-nusrah-front.

[13] *Id*.

[14] *Id*.

[15] DOJ, Press Release, "Fourth Brooklyn, New York, Resident Charged With Attempt and Conspiracy to Provide Material Support to ISIL," April 21, 2015. Available at https://www.justice.gov/opa/pr/fourth-brooklyn-new-york-resident-charged-attempt-and-conspiracy-provide-material-support.

[16] DOJ, Press Release, "Federal Jury Convicts Three Minnesota Men for Conspiring to Join ISIL and Commit Murder in Syria," June 3, 2016. Available at https://www.justice.gov/opa/pr/federal-jury-convicts-three-minnesota-men-conspiring-join-isil-and-commit-murder-syria.

[17] *Id*.

[18] *U.S. v. Hamza Ahmad*, et. al. (Complaint) (D. Minn. Feb. 4, 2015).

[19] *U.S. v. Ramiz Zijad Hodzic et al.*, (Indictment) (E.D. Mo., Feb. 5, 2015). Available at https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/02/09/certifiedcopyofindictment_comp.pdf.

[20] *Id*.

[21] *Id*.

[22] DOJ, Press Release, "Virginia Man Charged With Attempting to Provide Material Support to ISIL," Dec. 22, 2016. Available at https://www.justice.gov/opa/pr/virginia-man-charged-attempting-provide-material-support-isil-0.

[23] *Id*.

[24] As detailed in the statement of facts for the plea, the individual also wired a total of $550 to Abu Isa Al-Amriki, a now-deceased ISIS member, recruiter and external attack planner.[25] The individual further admitted to attempting to travel to Libya to join the ISIS regional affiliate there.[26]

Along with raising funds in the United States or through U.S. persons, ISIS financiers and supporters are seeking to access the U.S. and international financial systems, both directly and indirectly, to move funds in support of ISIS and its regional affiliates throughout the world. According to U.S. law enforcement, while some terrorists (especially core AQ operatives) have avoided using regulated financial institutions, as they believe law enforcement access to transactional information could be used to track their activities, some ISIS-inspired supporters have displayed less concern over operational security and are more willing to use regulated financial institutions.

U.S. authorities have also identified instances where ISIS operatives route transactions through third parties to avoid detection, as well as channel financial activity through neighboring localities (as ISIS operates in regions with limited access to the international financial system). Although U.S. financial institutions generally have effective suspicious activity monitoring systems in place, institutions may be unwittingly exposed to funds that originated with ISIS financial facilitators when they facilitate funds transfers through correspondent accounts.

For example, U.S. authorities have identified complicit foreign money remitters and exchange houses that have assisted ISIS in accessing the international financial system. On December 13, 2016, pursuant to Executive Order (E.O.) 13224, Treasury designated Iraq-based Selselat al Thahab Money Exchange, ISIS financier Fawaz Muhammad Jubayr al-Rawi, and his company, the Hanifa Currency Exchange in Albu Kamal, Syria, for playing an important role in ISIS's financial operations by helping the terrorist group move its money.[27] This included conducting more than 100 financial transfers into ISIS-controlled territory between April 2015 and March 2016.[28] The Hanifa Currency Exchange and Selselat al Thahab were also added to the United Nations (UN) ISIL and AQ Sanctions List on July 20, 2017, demonstrating strong multilateral agreement and action against these terrorist facilitators. Along with complicit foreign individuals and financial institutions, ISIS may also access the U.S. financial system by having ISIS supporters transfer funds through foreign banks that are not subject to the same or similar regulatory guidelines as U.S. banks, or do not have in place effective AML/CFT processes or controls.

Individuals acting on behalf of ISIS are also seeking to procure commercial and other goods from U.S. companies. In one case, a group of United Kingdom (UK)-based ISIS supporters allegedly purchased surveillance and thermal imaging equipment from a UK and Canadian

---

[24] DOJ, Press Release, "Columbus Man Pleads Guilty to Attempting to Provide Material Support to ISIS," July 6, 2017. Available at https://www.justice.gov/usao-sdoh/pr/columbus-man-pleads-guilty-attempting-provide-material-support-isis

[25] *U.S. v. Aaron T. Daniels* (Statement of Facts) (S.D. Ohio, June 6, 2017).

[26] *Id.*

[27] Treasury, Press Release, "Treasury Sanctions Senior Isil Financier and Two Money Services Businesses," Dec. 13, 2016. Available at https://www.treasury.gov/press-center/press-releases/Pages/jl0684.aspx.

[28] *Id.*

company using the name of the UK web development company where they were employed.[29] These goods were then provided to the company owner (who was an ISIS supporter) who had gone to Syria to join ISIS.[30] These individuals also unsuccessfully sought to procure surveillance and tracking equipment from a U.S.-based company.[31]

B. HIZBALLAH

Hizballah continues to present a significant terrorism threat to the United States and U.S. interests globally.[32] Hizballah receives the majority of its funding, upwards of $700 million a year, from the Iran.[33] Iran, the world's foremost state sponsor of terrorism, uses deceptive tactics including front and shell companies to exploit markets in numerous countries to fund its nefarious activities.[34] Iran's deceitful tactics include forging documents, obfuscating data, and hiding illicit activities under official cover of government entities, among many others.[35] This has included efforts by senior officials with the Central Bank of Iran (CBI) to conceal the true nature of transactions that were destined for Hizballah.[36] The objective is to ensure that no legitimate company or government knows that they are being used to achieve Iran's illicit aims.

In addition to funding from Iran, Hizballah receives millions of dollars from a global network of supporters and businesses.[37] These supporters generate funds from both legitimate and illicit activities (much of which is not directly connected to Hizballah or done at the behest of Hizballah) and send funds to Hizballah operatives using a variety of funds transfer methods, including banks, money remitters, and cash. Hizballah also uses a far-flung network of companies and brokers to procure weapons and equipment and clandestinely move funds on behalf of operatives and its overseas activities.[38]

Because of this global presence, including financial support from Lebanese diaspora communities in West Africa, South America, and other jurisdictions, Hizballah is more reliant on having access to the international financial system. Such access is facilitated by the fact that Hizballah, unlike AQ or ISIS, is not subject to UN sanctions, and many countries have not designated the entirety of Hizballah under their own domestic authorities or imposed other restrictions on Hizballah-financial transactions.

Hizballah operatives are active in the United States and are looking to raise funds through donations, commercial activity, and criminal activity. For example, on March 24, 2017, U.S. authorities arrested Kassim Tajideen on charges of evading U.S. sanctions and money

---

[29] *In the Matter of the Search of Electronic Account Stored at Premises Controlled and Hosted by Facebook headquartered in Menlo Park, California, et. al.* (N.D. Ca. Dec. 9, 2016).
[30] *Id*.
[31] *Id.*
[32] Worldwide Threat Assessment.
[33] Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence, Speech before the Foundation for the Defense of Democracies, June 5, 2018. Available at https://home.treasury.gov/news/press-releases/sm0406.
[34] *Id*.
[35] *Id*.
[36] *Id*.
[37] Treasury, Press Release, "Treasury Targets Hizballah Financial Network in Africa and the Middle East," Available at https://home.treasury.gov/news/press-releases/sm0278
[38] *Id*.

laundering.[39] Tajideen is a prominent financial supporter of Hizballah who was designated as a specially designated global terrorist (SDGT) in 2009.[40] In response to the designation, Tajideen allegedly restructured his multi-million dollar business empire in order to evade the U.S. sanctions and continue conducting transactions with U.S. entities and shipping goods from U.S. ports in support of Tajideen's commercial activities.[41]

Hizballah members and supporters have also used criminal activity to generate funds, some of which are then provided to Hizballah. In October 2015, U.S. authorities conducting a two-year undercover investigation arrested a woman in Atlanta, Georgia.[42] She was charged in New York, where her case is pending, with conspiracy to launder funds she believed to be drug money, and arranging for the sale of thousands of firearms, including military assault rifles, machine guns, and sniper rifles, to criminal groups in Iran and Lebanon, including Hizballah.[43] Her co-conspirator, an alleged attorney who claimed to have connections to Hizballah and to banks in the Middle East and Europe, was arrested in Paris.[44] After extradition from France, the co-conspirator pled guilty to a money laundering conspiracy charge and was sentenced to twenty months in prison, three years of supervised release, and a penalty of forfeiture.[45]

According to U.S. law enforcement, Hizballah supporters continue to procure dual-use goods and other military and commercial equipment from U.S. companies to support Hizballah terrorist activities. For example, in February 2018, U.S. authorities indicted three individuals for conspiring to illegally export goods and technology from the United States to Lebanon and to Hizballah.[46] The three individuals allegedly conspired to purchase from a U.S. company certain unmanned aerial vehicle (UAV) components and other controlled goods, then after providing false information to the U.S. company so the company could obtain appropriate authorization for export, exporting the goods to a third country before eventually shipping them on to Lebanon.[47]

C. AQ

AQ and its regional affiliates, including AQAP as well as other terrorist groups associated with

---

[39] DOJ, Press Release, "Lebanese Businessman Tied to Hizballah Arrested for Violating and Defrauding the U.S. Government," March 24, 2017. Available at https://www.justice.gov/opa/pr/lebanese-businessman-tied-hizballah-arrested-violating-ieepa-and-defrauding-us-government.

[40] Treasury, Press Release, "Treasury Targets Hizballah Financial Network," Dec. 9, 2010. Available at https://www.treasury.gov/press-center/press-releases/Pages/tg997.aspx. According to the press release, Tajideen allegedly used profits from his businesses to support Hizballah.

[41] DOJ, Press Release, "Lebanese Businessman Tied to Hizballah Arrested for Violating and Defrauding the U.S. Government," March 24, 2017. These transactions included at least 47 individual wire transfers, totaling approximately $27 million, to parties in the U.S to facilitate Tajideen's commercial activities.

[42] DOJ, Press Release, "Two Hezbollah Associates Arrested On Charges Of Conspiring To Launder Narcotics Proceeds And International Arms Trafficking," October 9, 2015. Available at https://www.justice.gov/usao-edny/pr/two-hezbollah-associates-arrested-charges-conspiring-launder-narcotics-proceeds-and

[43] *Id*.

[44] *Id*.

[45] *Id*.

[46] DOJ, Press Release, "Two Men Arrested And Charged With Illegally Exporting UAV Parts And Technology To Hizballah," Feb. 16, 2018. Available at https://www.justice.gov/usao-mn/pr/two-men-arrested-and-charged-illegally-exporting-uav-parts-and-technology-hizballah.

[47] *Id*.

AQ, such as ANF, continue to pose a threat to the United States and its allies.[48] AQ and its regional affiliates have historically generated almost all of their revenue from outside the United States, such as from individual fundraisers in Gulf countries, and their operatives and supporters are located throughout the world, including in Afghanistan, Pakistan, East Africa, Southeast Asia, and increasingly in Yemen and Syria, requiring them to move funds between these jurisdictions.[49]

While the rise of ISIS has deprived AQ and its regional affiliates of some supporters and operatives, limited fundraising on behalf of AQ and its regional affiliates continues to occur in the United States. On April 12, 2018, three U.S. - based individuals[50] pleaded guilty to concealing the provision of thousands of dollars to SDGT Anwar Al-Awlaki, a member of AQAP.[51] According to court documents, they allegedly collected and sent several thousand dollars to associates of Al-Awlaki using a combination of bank transfers and MSB transactions as well as traveling overseas with cash.[52] Two of the individuals also allegedly obtained funds by opening credit cards with financial institutions and withdrawing money with no intention of repaying the amounts obtained.[53]

While supporters of AQAP in the United States collect funds using a variety of financial channels, they are more likely to send funds out of the U.S. through MSBs or travel and carry cash. Additionally, when these groups transfer funds between regional affiliates outside of the U.S., those funds may indirectly be routed through the U.S. financial system because they are processed through U.S. banks or MSBs, although neither the ultimate originator nor beneficiary is in the United States.

Along with AQAP, supporters of ANF have also sought to raise funds in the United States. Methods of fundraising have included direct solicitations via social media (where funds are sent through a variety of channels, including banks, MSBs, and online payment systems), seeking funds under the false pretenses of charity, and low-level criminal activity. For example, on December 17, 2014, an individual was sentenced for conspiring to provide material support to several FTOs, including AQ, ANF, and Al-Shabaab.[54] According to the indictment, the individual, working with a co-conspirator, sent funds (via an MSB) on several occasions to what

---

[48] Worldwide Threat Assessment.
[49] Daniel Glaser, Assistant Secretary for Terrorist Financing, Testimony before the House Committee on Foreign Affair's Subcommittee on Terrorism, Nonproliferation, and Trade, and House Committee on Armed Services' Subcommittee on Emerging Threats and Capabilities, June 9, 2016.
[50] A fourth individual pleaded guilty on July 10, 2017 to one count of conspiracy to provide and conceal material support or resources to terrorists and one count of solicitation to commit a crime of violence. DOJ, Press Release, "Man Pleads Guilty to Conspiring to Provide Material Support to Terrorists and Soliciting the Murder of a Federal Judge," July 10, 2017.
[51] DOJ, Press Release, "Three Men Plead Guilty to Concealing Sending Funds to Anwar Al-Awlaki," Apr. 12, 2018. Available at https://www.justice.gov/opa/pr/three-men-plead-guilty-concealing-sending-funds-anwar-al-awlaki. Al-Awlaki is confirmed to have died on September 30, 2011 in Yemen.
[52] U.*S. v. Yahya Farooq Mohammad*, (Indictment) (N.D. Ohio, September Sept. 30, 2015). Available at https://www.justice.gov/opa/file/790971/download.
[53] *Id*.
[54] DOJ, Press Release, "Defendant Sentenced for Conspiring to Provide Material Support to Foreign Terrorist Organizations," Dec. 17, 2014. Available at https://www.justice.gov/opa/pr/defendant-sentenced-conspiring-provide-material-support-foreign-terrorist-organizations.

he thought was an ANF supporter.[55] The individual indicated the funds were to be used to purchase weapons and supplies for ANF in Syria, and for attacks against U.S. interests.[56]

Individuals acting on behalf of ANF have also sought to procure tactical equipment and other sensitive goods from U.S. companies to support terrorist activity in Syria. For example, on January 15, 2016, a Syrian-born naturalized U.S. citizen pleaded guilty to conspiring to export U.S.-origin goods from the United States to Syria to support Ahrar al-Sham and other insurgent groups in Syria, in violation of U.S. sanctions.[57] According to court documents, this U.S. citizen and his co-conspirators purchased tens of thousands of dollars-worth of goods from companies and vendors in the United States, consisting largely of tactical equipment such as sniper rifle scopes, night vision rifle scopes, night vision goggles, laser bore sighters, speed loaders and bullet proof vests, then traveled with the goods aboard commercial flights to Turkey and transported the goods into Syria or provided them to others for transport.[58]

D. AL-SHABAAB

Al-Shabaab continues to exploit Somali diaspora communities in the United States to raise funds to support terrorist activities in Somalia and East Africa.[59] Some U.S.-based Al-Shabaab fundraisers have explicitly solicited funds for Al-Shabaab's terrorist activities, while others have used false charitable pretenses and then diverted the funds to Al-Shabaab. These funds are primarily sent through MSBs, as Al-Shabaab supporters and facilitators in the U.S. are more likely to send funds out of the U.S. through MSBs than other payment channels.

For example, on October 25, 2016, Muna Osman Jama and Hinda Osman Dhirane were convicted for providing material support to Al-Shabaab.[60] They sent money to Al-Shabaab financiers in Somalia and Kenya.[61] These transfers, totaling approximately $5,000 and sent via MSBs, were broken down into small amounts as low as $50 or $100.[62] The defendants also organized women from Somalia, Kenya, Egypt, the Netherlands, Sweden, the UK, and Canada, as well as Minneapolis to raise funds for Al-Shabaab.[63] They met regularly in a private chatroom that Jama established to raise funds and send the money to Somalia and Kenya to finance Al-Shabaab military operations and safe houses.[64]

---

[55] *U.S. v. Gufran Ahmed Kauser Mohammed*, (Indictment) (S.D. Fla. May 21, 2013).
[56] *Id*.
[57] *U.S. v. Amin al-Baroudi*, (Statement of Facts) (E.D. Va., January Jan. 15, 2016). Available at https://www.justice.gov/opa/file/813586/download.
[58] *Id*.
[59] Prior to Syria's emergence as the preeminent destination for aspiring U.S. FTFs, Somalia had been a popular conflict zone for U.S. those few U.S. persons seeking to travel overseas and support terrorist groups. Beginning in 2010, the rate of attempted and successful travel steeply declined. DHS, Reference Aid: US Foreign Fighters.
[60] DOJ, Press Release, "Two Women Found Guilty of Providing Material Support to Terrorists," October Oct. 25, 2016. Available at https://www.justice.gov/usao-edva/pr/two-women-found-guilty-providing-material-support-terrorists.
[61] *U.S. v. Muna Osman Jama et al*, (Superseding Indictment) (E.D. Va. June 26, 2014). Available at https://www.justice.gov/usao-edva/press-release/file/904951/download.
[62] *Id*.
[63] *Id*.
[64] *Id*.

E. OTHER TERRORIST GROUPS AND RADICALIZED INDIVIDUALS

In addition to the groups identified above, supporters of other terrorist organizations located outside of the United States may engage in TF activity in the United States. While these groups may be less active in the United States than those identified above, their supporters may still seek to raise funds from U.S.-based supporters or move funds through the U.S. financial system, or potentially purchase weapons or material from U.S.-based companies for terrorist operations outside of the United States.

While the Taliban generates the vast majority of its revenue outside the United States, specifically from its activities in Afghanistan and Pakistan, as well as from fundraising activity in the Gulf, there have been some past cases of U.S.-based Taliban supporters raising funds in the U.S. to support the Taliban as well as other terrorist groups based in Pakistan and Afghanistan. For example, Agron Hasbajrami was sentenced to 16 years in prison on August 13, 2015 for providing material support to terrorists, which included sending $1,000 in multiple wire transfers abroad to support terrorist activities in Pakistan and Afghanistan, including the Pakistani Taliban.[65]

Historically, the Revolutionary Armed Forces of Colombia (FARC) has utilized drug trafficking with a U.S. nexus to finance their terrorist activities, as well as using intermediaries to launder funds associated with drug trafficking through the U.S. financial system. For example, Faouzi Jabar, who pleaded guilty in July 2017 to providing material support to the FARC, also agreed to assist with the transportation and storage of FARC-owned cocaine in West Africa, and with the laundering of cocaine proceeds for the FARC, including by moving the cocaine proceeds through bank accounts in New York.[66] However, given the November 2016 peace accord with the Colombian government and the resulting efforts by the FARC to transition to a political party, the TF threat posed by the FARC to the U.S. financial system is somewhat more limited than in the past. In addition to the Taliban and FARC, U.S. authorities have previously identified U.S.-based financial activity involving Hamas, Lashkar-e Tayyiba (LeT), and the Islamic Movement of Uzbekistan.

U.S. authorities have also identified instances where radicalized individuals based in the United States have purchased ammunition, firearms, tactical gear or equipment, and materials used to make explosive devices that were later used in a terrorist attack in the United States. These individuals have been both returning FTFs and individuals who are inspired by ISIS to carry out a terrorist attack but are not directly associated with ISIS.[67] Ahmad Rahimi, who was convicted of criminal charges related to his execution and attempted execution of bombings in New York City on September 17, 2016, purchased on an online marketplace several items commonly used

---

[65] DOJ, Press Release, "Albanian National Sentenced to 16 Years for Attempting to Support Terrorism," Aug. 13, 2015. Available at https://www.justice.gov/opa/pr/albanian-national-sentenced-16-years-attempting-support-terrorism; *U.S. v. Agron Hasbajrami,* (Sentencing Memorandum) (E.D.N.Y. Aug. 11, 2015).
DOJ, Press Release, "Ivorian Man Pleads Guilty In Manhattan Federal Court To Conspiring To Provide Material Support To The FARC," July 25, 2017. Available at https://www.justice.gov/usao-sdny/pr/ivorian-man-pleads-guilty-manhattan-federal-court-conspiring-provide-material-support.

[67] Christopher Wray, FBI Director, Testimony before the House Committee on the Judiciary, "Oversight of the Federal Bureau of Investigation," Dec. 7, 2017. Available at https://judiciary.house.gov/wp-content/uploads/2017/12/Director-Wray-Testimony.pdf.

in improvised explosive devices, including citric acid, ball bearings, circuit boards and electric igniters.[68] Christopher Lee Cornell, who pleaded guilty to criminal charges in connection with plotting, planning and attempting an attack on government officials during the State of the Union Address in 2015 in the name of ISIS, used money from his personal savings to purchase two semi-automatic rifles and 600 rounds of ammunition for $1,900 that were to be used in the attack.[69]

[68] *U.S. v. Ahmad Khan Rahimi*, (Sentencing Memorandum) (S.D.N.Y, Jan. 16. 2018).
[69] *U.S. v. Christopher Lee Cornell,* (Sentencing Memorandum) (S.D. Ohio, Nov. 21, 2016).

SECTION 2. VULNERABILITIES AND RISKS

A. BANKS

The banking system remains an attractive means for terrorist groups seeking to send money globally because of the speed and ease at which they can move funds, as well as the large volume of transactions that are processed daily. Other financial institutions such as MSBs also rely on banks to conduct cross border transactions. In the United States depository institutions filed approximately 33 percent of the 6,000 Suspicious Activity Reports (SARs) filed for TF in 2015, 2016, and 2017 and approximately 60 percent of SARs associated with U.S.-based individuals charged with supporting terrorist activity.[70] An analysis of those SARs associated with U.S.-based individuals charged with supporting terrorist activity found that these funds were most commonly used to support terrorist groups overseas or to support foreign travel or travel-related purchases, and most SARs were filed based on derogatory information regarding the sender or recipient, rather than based on suspicious activity associated with the transaction.[71]

U.S. banks, particularly large dollar-clearing banks operating on a global scale, play an integral role in facilitating global finance and trade, specifically by providing U.S. dollar clearing services through cross-border banking relationships. This activity, and the sheer volume and diversity of international financial transactions that are processed, which may expose U.S. banks to unknowingly moving funds that are associated with or ultimately destined for a terrorist or terrorist group. This can occur when U.S. banks clear U.S.-dollar transactions on behalf of foreign correspondents that are not subject to the same or similar regulatory guidelines as U.S. banks, or do not have in place effective AML/CFT processes or controls. This may be especially true where a foreign financial institution, based on its particular risk profile (which may include geographic profile, business line, or customer base), does not implement effective customer due diligence practices, suspicious activity identification processes, and/or recordkeeping processes.[72] This lack of effective AML/CFT controls increases the likelihood that funds associated with illicit finance, including TF, may flow through these accounts and into the U.S. financial system.

To mitigate this risk, the federal functional regulators require U.S. banks to conduct due diligence on their foreign correspondents to ensure that the foreign correspondent's controls are adequate to manage the risk. Additionally, most U.S. banks have developed sophisticated internal programs and models to identify potential TF, resulting in highly useful SARs that have supported multiple actions to disrupt terrorism and TF activity over the years. Robust implementation of these and other AML/CFT controls across U.S. financial institutions has made operating within the regulated financial system more risky, costly, time intensive and difficult for

[70] FinCEN SAR Stats, available at https://www.fincen.gov/reports/sar-stats; Information derived from an analysis of financial institution BSA reporting.
[71] Information derived from an analysis of financial institution BSA reporting.
[72] For example, the New York State Department of Financial Services (DFS) identified several "serious and persistent" AML/CFT deficiencies for the New York branch of Habib Bank Limited (HBL), Pakistan's largest bank. These included, among others, HBL's failure to screen at least $250 million in transactions routed through its New York Branch that should have been identified as high-risk, including transactions that involved the leader of a Pakistani terrorist group and an individual designated as a SDGT. See *New York Department of Financial Services, In the Matter of Habib Bank Limited and Habib Bank Limited, New York Branch* (Statement of Charges), ¶ 18-19 (Aug. 24. 2017).

TF networks.

U.S. banks may become vulnerable to unknowingly moving funds affiliated with terrorism when a foreign correspondent bank provides services to other financial institutions that may have branches or facilities in or near a territory where terrorist groups are active. As ISIS operates in regions with limited access to the international financial system, ISIS financial operatives may attempt to directly and indirectly channel financial activity through banks or other financial institutions in neighboring localities.[73]

In some cases, terrorists or their supporters overseas may seek to move funds and obfuscate their involvement by collaborating with witting supporters or facilitators who own or control foreign non-bank financial institutions, such as exchange houses. These funds can flow through the U.S. financial system when U.S. banks acting as correspondents process transactions from foreign banks that are ultimately on behalf of complicit institutions or individuals (i.e. when the U.S. bank serves as an intermediary and does not have a direct relationship with the ordering customer or the ultimate beneficiary or both). For example, on June 15, 2017, OFAC designated Umar al-Kubaysi, an Iraqi citizen, and his company, Al-Kawthar Money Exchange for providing support to ISIS.[74] Between late 2015 and early 2016, Al-Kawthar Money Exchange reconciled financial transfers worth approximately $2.5 million with another Iraq-based money exchange company that was associated with ISIS financial facilitators.[75] Al-Kawthar sent transfers using a Gulf-based company, which is co-owned by two suspected ISIS facilitators.[76] Al-Kawthar had also facilitated money transfers for AQ in Iraq, one of the names ISIS used to be known by, in 2013.[77]

U.S. banks are also vulnerable to TF because of the limited use and uneven implementation of U.N counterterrorism sanctions[78] by foreign governments and foreign financial institutions. These measures are a critical tool for identifying and disrupting the financial networks of terrorist organizations, as well as serving as a valuable source of information on individuals or entities who may be linked to TF or terrorism. For example, individuals linked by familial or corporate ties to designated persons may execute funds transfers on their behalf following designation. Additional identifying information on those who have relationships with designated persons can further enable transaction screening and monitoring systems to identify those who may act on their behalf, improving the ability of U.S. and foreign banks to detect TF-related

[73] FATF, Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL) at 27, February 2015. Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.
[74] Treasury, Press Release, "Treasury Sanctions Iraq-Based ISIS Financial Facilitation Network," June 15, 2017. Available at https://www.treasury.gov/press-center/press-releases/Pages/sm0109.aspx.
[75] *Id*.
[76] *Id*.
[77] *Id*. U.S. authorities have identified similar attempts by complicit third-country exchange houses or trading companies acting as money transmitters to process funds transfers through the United States in support of business with Iran that is not exempt or otherwise authorized by OFAC. See OFAC, Advisory, "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran," Jan. 10, 2013. Available at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110_iran_advisory_exchange_house.pdf.
[78] This refers to UN listings made pursuant to United Nations Security Council Resolutions (UNSCRs) 1267/1989/2253 and 1988, as well as autonomous national or supranational designations made pursuant to UNSCR 1373.

transactions. However, the effectiveness of sanctions in protecting the U.S. and international financial system from abuse is limited by the fact that many foreign governments do not often publicly identify or sanction terrorists and their support networks.[79] While the UN is able to publicly identify and sanction some terrorist support networks , such as Kubaysi and his company, Al-Kawthar Money Exchange, referenced above (because of their ties to ISIS), this is not routine for many U.S. designations. While many foreign governments have the legal framework to domestically designate terrorist support networks, they often lack either the political will or resources to do so. A separate challenge is financial activity associated with Hizballah, which uses the international financial system more regularly than other terrorist groups. As noted above, Hizballah is not listed at the UN and is not domestically designated as a terrorist organization by a significant number of foreign jurisdictions.

While the U.S. has maintained a robust sanctions program and broad primary embargo against Iran, which has made it difficult for Iranian-linked entities to conduct TF-related activities with a U.S. nexus, Iran's use of deceptive practices to access the international financial system and limited measures taken by some foreign jurisdictions to address Iran's support to terrorism may expose U.S. banks to indirectly and unknowingly moving funds linked to Iran's terrorist proxies.

This is made all the more challenging by CBI's complicity in supporting the financing of terrorism. In one case, the CBI's Governor, Valiollah Seif, other CBI officials, and the Qods Force teamed up to take advantage of Iraq's banking sector in order to surreptitiously move funds on behalf of the Qods Force and Hizballah.[80] As part of this scheme, Seif, along with the assistant director of the CBI's International Department, conspired with the Qods Force to conceal the movement of millions of dollars in multiple currencies through the international financial system, including through Iraqi banks.[81] Seif used his influence and credentials as the head of CBI to conceal the true nature of transactions that were destined for the Qods Force and its proxy, Hizballah.[82] The Chairman and Chief Executive of Al-Bilad Islamic Bank, an Iraqi bank, acted as an intermediary to enable and conceal the Qods Force's exploitation of Iraq's banking sector to send funds to Hizballah.

Another sanctions-related vulnerability involves designated terrorist supporters surreptitiously accessing the U.S. financial system through the use of non-transparent foreign legal entities. However, the misuse of foreign legal entities solely to move funds is rare among individuals/entities designated for support to terrorism, and where it has been observed, it has usually been associated with the purchase of goods from U.S.-based companies.

An additional challenge for financial institutions is that many transactions associated with terrorism or TF are often hard to distinguish from legitimate day-to-day transactional activity. An assessment of SARs associated with U.S.-based individuals charged with supporting terrorist

[79] For example, a 2015 report from the FATF found that only nine percent of the 194 jurisdictions in the FATF global network had proposed a designation to the UN Sanctions Committees, and only 16 percent had made national designations pursuant to UNSCR 1373. See FATF, Terrorist Financing: FATF Report to G20 Leaders, Nov. 2015, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-financing-actions-taken-by-FATF.pdf.
[80] Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence, Speech before the Foundation for the Defense of Democracies, June 5, 2018
[81] *Id*.
[82] *Id*.

activity found that most were filed based on derogatory information regarding the sender or recipient, rather than based on suspicious activity associated with the transaction.[83] U.S. authorities are working to address this challenge through regular engagement and information sharing with U.S. banks, including through the dissemination of contextual information about a customer's behavior, account activity and geographic risk, that when combined with other information available to financial institutions, can assist banks in identifying potential TF activity.[84] Nonetheless, identifying TF transactions remains an evolving challenge for both U.S. authorities and financial institutions.

U.S. banks face the risk that they may inadvertently conduct transactions on behalf of terrorist financiers overseas who use foreign correspondent banks in jurisdictions that may not be subject to the same or similar regulatory requirements as U.S. banks; that do not have in place effective AML/CFT processes or controls; or that serve individuals knowingly sending funds on behalf of terrorists or terrorist groups.

B. REGULATED MSBS

Licensed MSBs can also be vulnerable to abuse for terrorist financing.[85] The MSB industry in the United States is broad and diverse and plays an essential role in financial inclusion; over one-quarter of U.S. households use non-bank financial institutions, including money transmitters. Similar to banks, licensed MSBs, especially those that have a large number of foreign agents and affiliates, can unknowingly provide terrorists and their supporters a channel to move funds fairly quickly and efficiently through the international financial system. It is important to note that these large multinational MSBs, consistent with their identified TF risk, have developed sophisticated internal programs and models to identify potential TF, resulting in highly useful SARs that have supported multiple actions to disrupt terrorism and TF activity.

MSBs filed approximately 58 percent of the approximately 6,000 SARs flagged for TF between 2015 and 2017, and approximately 30 percent of SARs associated with U.S.-based individuals charged with supporting terrorist activity.[86] The high percentage of overall SARs is due to the fact that the largest money transmitters have a large global footprint and because their vast international networks of agents have visibility into both sides of a transaction that may not include U.S. persons, something U.S. banks may not have. An analysis of those SARs associated with U.S.-based individuals charged with supporting terrorist activity found that these funds 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), and were filed based on derogatory information regarding the sender or recipient, not from suspicious activity linked to

[83] Information derived from an analysis of financial institution BSA reporting. Some SARs on suspected terrorists are filed for other suspicious activity, such as ML

[84] For example, FinCEN has issued four non-public advisories to financial institutions highlighting specific contextual factors and information that may indicate TF, and U.S. law enforcement regularly engages U.S. banks and other financial institutions with typologies and other information developed from recent investigations.

[85] FATF, Emerging Terrorist Financing Risks at 21, October Oct. 2015. Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.

[86] FinCEN SAR Stats; Information derived from an analysis of financial institution BSA reporting. Some SARs included detailed information on a subject's potential link from terrorist activity, such as from the subject's social media postings.

terrorism.[87]

MSBs are used frequently among certain terrorist groups, such as Al-Shabaab and other AQ affiliates.[88] 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.[89]

MSBs in the United States are vulnerable to abuse for TF because (i) they may unknowingly move funds on behalf of terrorists and their supporters, and (ii) complicit employees or owners willingly facilitate TF in violation of applicable laws, regulations and the MSB's own AML/CFT policies and procedures. Similar to banks, many of the funds transfers sent through MSBs associated with TF or terrorism do not reflect suspicious activity that would indicate a link to terrorism, and most SARs identifying TF activity are filed based on derogatory information, although some are filed for suspicious activity other than terrorism.

Along with unknowingly moving funds on behalf of terrorists, there is also the continued risk that U.S.-based complicit employees or owners may misuse MSBs to transfer funds on behalf of illicit actors, including terrorist groups. This risk is more 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. In one past case, an individual raised funds for Al-Shabaab and collaborated with an MSB employee who helped the individual avoid leaving a paper trail by structuring transactions into low dollar amounts and by using false identification information.[90]

Additionally, MSBs are required to collect customer identification information for funds transfers $3,000 or above. While collection of this information is not required for transactions below that threshold, in practice the largest MSBs have internal policies that require the collection of customer information well below this threshold.[91] MSBs (along with other FIs) are also required to file SARs when there is suspicion of ML or TF, regardless of threshold. An assessment of SARs associated with U.S.-based individuals charged with supporting terrorist activity found that 94 percent of the SARs filed by MSBs involved suspicious transactions under $800, indicating that MSBs are collecting customer information and filing SARs on suspected TF well below the $3,000 threshold.[92] Thus, while the current $3,000 recordkeeping threshold results in the processing of some funds transfers by MSBs without verifying customer identification, and these low value transactions by occasional customers presents a manageable

---

[87] *Id*.

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

[89] According to an analysis of financial institution reporting related to ISIS filed between 2014 and 2016, MSBs accounted for 66 percent of SARs, but only 1.3 percent of funds. Banks accounted 33 percent of SARs but 98 percent of funds.

[90] See *U.S. v. Mohamud Abdi Yusuf, et al*. (E.D. Mo. October 2010). Available at https://archives.fbi.gov/archives/stlouis/press-releases/2012/minneapolis-man-receives-three-years-probation-for-structuring-financial-transactions.

[91] 31 C.F.R. § 1010.410(e).

[92] An assessment of SARs associated with U.S.-based individuals charged with supporting terrorist activity found that 94 percent of the SARs filed by MSBs involved suspicious transactions under $800. Information derived from an analysis of financial institution BSA reporting.

TF risk.

In addition to unknowingly moving funds on behalf of terrorists, and complicit employees knowingly facilitating TF, some MSBs that engage in online person-to-person funds transfers have not maintained adequate AML/CFT controls. The lack of effective controls has allowed terrorist financiers to move funds on these platforms. For example, in one case, a U.S.-based online MSB entered into a Settlement Agreement with OFAC for, among other things, transferring several thousand dollars on behalf of an SDGT.[93]

For MSBs, the primary TF risk is linked to funds being moved from the U.S. on behalf of ISIS and its regional affiliates, AQ and its regional affiliates, and U.S.-based FTFs who may be seeking to join these or other terrorist groups. Licensed MSBs may also be misused by complicit employees who willingly facilitate TF in violation of applicable laws and regulations and the MSBs own AML/CFT policies and procedures.

C. UNLICENSED MONEY TRANSMITTERS

Despite the requirements to register with the federal government before providing money transfer services and requirements for licensing in almost all U.S. states, some individuals and entities provide funds transfer and other financial services in the U.S. but do not comply with licensing and regulatory requirements. SARs filed by banks citing potential unlicensed money transmission activity as well as civil enforcement actions by FinCEN identified a variety of businesses, including grocery or convenience stores, gas stations, and liquor stores, which have operated as unlicensed money transmitters.

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 AQAP (Yemen), and the Taliban, than other terrorist groups. They may also be facilitating transactions for ISIS, its regional affiliates and non-bank financial institutions, such as exchange houses, that transfer funds on their behalf. While a review of law enforcement and regulatory actions indicates that the vast majority of unlicensed money transmitters identified by law enforcement are not involved in financing terrorism, those unlicensed money transmitters linked to TF had the following characteristics:

- The individual operators were linked to persons overseas, including in jurisdictions at high-risk for ML or TF;
- The business was linked to used car dealers or cash intensive businesses; or
- The individual operators or businesses were linked to identified terrorist supporters or facilitators.

For example, Saifullah Anjum Ranjha, a Pakistani national residing in the United States who operated a unlicensed money transmission business, agreed to transfer funds that he was told were derived from a variety of illicit activities, including international drug trafficking,

[93] OFAC, *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and PayPal, Inc*., March 25, 2015. Available at https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150325_33.aspx.

international smuggling of counterfeit cigarettes and weapons, as well as funds associated with AQ.[94] These funds were sent to recipients in several countries, including those identified as being high-risk for ML/TF.

For the U.S. authorities, the TF risk involving unlicensed money transmission 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 the Taliban.

U.S. regulatory and law enforcement authorities recognize the risk posed by unlicensed money transmission and have aggressively targeted these actors for investigation and prosecutions, with a focus on the most significant violators. This has been especially important in terrorism cases, where criminal penalties for the act of engaging in unlicensed money transmission offer law enforcement and prosecutors a powerful tool to sanction violators where proving the connection to TF may be difficult or pose particular evidentiary challenges. In addition to prosecuting unlicensed money transmitters, the U.S. government has also worked with financial institutions to more effectively detect and report potential unlicensed money transmission. For example, FinCEN has issued detailed advisories to financial institutions on how to report suspicious activity associated with illegal MSBs.

D. CASH SMUGGLING AND U.S. DOLLAR ACTIVITY OVERSEAS

While the cross-border transportation of cash, when subject to appropriate AML/CFT controls, including the filing of required declarations, can be used as a legitimate method to settle payments and transfer funds, U.S. authorities have identified cross-border cash transactions, both below and above applicable reporting thresholds, as an important channel for terrorists and their supporters to move funds from the United States to support operations overseas. Robust implementation of AML/CFT controls across financial institutions has made operating within the regulated financial system more risky, costly, time intensive and difficult for TF networks, making cash smuggling an increasingly attractive way for foreign terrorists to transfer funds. The use of cash is attractive to criminals mainly because of its anonymity, portability, liquidity and lack of audit trail.

U.S. authorities have identified U.S.-based terrorist financiers supporting a variety of foreign terrorist organizations moving funds in cash, as well as U.S.-based FTFs who travel overseas with cash. For example, U.S. authorities charged an individual in December 2017 with bank fraud and money laundering, the proceeds of which were allegedly used to support a designated terrorist organization.[95] This individual was caught with approximately $9,500 in cash when

[94] FBI, Press Release, "Pakistani National Pleads Guilty to Conspiracy to Operate an Unlicensed Money Remitting Business," February 5, 2009. Available at https://archives.fbi.gov/archives/baltimore/press-releases/2009/pakistani-national-pleads-guilty-to-conspiracy-to-operate-an-unlicensed-money-remitting-business.

[95] DOJ, Press Release, "Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists," December 14, 2017. Available at https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists.

attempting to board a flight to leave the United States.[96] When arrested, the individual allegedly admitted carrying $9,500 to avoid currency reporting requirements.[97]

Iran has also sought to access U.S. dollars to fund its terrorist proxies. In one case, using six front companies and with the help of the CBI, an extensive currency exchange network in Iran and the United Arab Emirates (UAE) exploited the UAE's currency exchange market to procure and transfer millions in U.S.-dollar denominated bulk cash.[98] It did this for the Qods Force, which has been designated by the United States and the European Union, to fund the Qods Force's malign activities and regional proxy groups by concealing the purpose for which the U.S. dollars were acquired.[99] In order to conceal Iran's involvement and these illicit activities from UAE authorities, the network forged documents and purposively disguised its conduct behind seemingly legitimate businesses, hiding its illicit activities through front and shell companies.

It is difficult – if not impossible – to completely stop the use of cash smuggling, and it remains a TF risk. Combined with the widespread demand for U.S. currency globally, multiple terrorist groups, including ISIS and its regional affiliates, AQ and its regional affiliates, ANF, Al-Shabaab and Hizballah, will continue to use cash smuggling as a less efficient alternative for moving funds globally.

E. CHARITABLE ORGANIZATIONS AND EXPLOITATION OF CHARITABLE CAUSES

The U.S. government recognizes and supports the important role charities play in delivering aid to communities worldwide. The U.S. government also recognizes that the vast majority of charities fully comply with the law and properly support only charitable and humanitarian causes. In addition, the U.S. government does not view the charitable sector as a whole as presenting a uniform or unacceptably high risk of being used or exploited for money laundering, terrorist financing, or sanctions violations.

The TF risk for charitable organizations in the United States can vary dramatically depending on the operations, activities, leadership and affiliations of the charitable organization. U.S. charities increasingly utilize a range of risk mitigation measures to limit and manage possible TF risks, including governance, transparency, accountability, and due diligence measures. The vast majority of the approximately one million charitable organizations in the U.S. that have been determined by the IRS to be tax-exempt generally face and present little TF risk. In fact, those U.S. charities that operate and provide funds solely domestically face low TF risk.[100] However, those U.S. charities that operate abroad, provide funding to, or have affiliated organizations in conflict regions, can face potentially higher TF risks.

---

[96] *Id*; *U.S. v. Zoobia Shahnaz*, (Proffer) (E.D. N.Y. Dec. 14, 2017).
[97] *Id*.
[98] Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence, Speech before the Foundation for the Defense of Democracies, June 5, 2018.
[99] *Id*.
[100] In 2014, of the approximately 1 million tax-exempt charitable organizations in the U.S., less than 10,000 had overseas activities (either in terms of programs or funds transfers) that would require them to file Schedule F along with their IRS Form 990. Many of the organizations that did file Form 990 were not active near conflict zones.

Targeted enforcement and prosecutions, focused oversight by regulators, sustained outreach, self-regulation initiatives within the charitable sector, and extensive domestic and international engagement and cooperation have reduced the ability of U.S. charitable organizations to be abused to facilitate financial or other material support for terrorist groups.

The ability to detect terrorist abuse and misuse of charities is facilitated by government reporting requirements and regulatory oversight. For example, charities provide specific information on the IRS Form 990 annually regarding their stated mission, programs, finances (including noncash contributions), donors, activities, and funds sent and used abroad. In addition, the extensive Schedule F of Form 990 includes many categories of reporting requirements for charities with overseas activities. In addition to Federal oversight, U.S. States oversee the practices of charities domiciled/operating in their jurisdictions.

However, there remains a TF risk for U.S. tax-exempt charitable organizations operating in, sending funds to, or with affiliated organizations in high-risk areas where ISIS and its regional affiliates, AQ and its regional affiliates, and other terrorist groups are most active, such as Afghanistan, Pakistan, Somalia, Syria, and Yemen. This risk highlights the importance of maintaining transparency and accountability of charitable funding and operations, such as internal controls and procedures, including end-use monitoring systems, to prevent the misuse of funding or services, to manage the remaining TF risks.

Internationally, recent actions against non-profit organizations located and operating outside of the United States demonstrate the continued risk the global charitable sector faces from abuse or misuse by terrorist organizations, even if the vast majority of U.S. charities face little TF risk. Terrorist supporters abuse charitable organizations abroad as a cover to raise and move funds, personnel, military supplies, and other resources, as well as to dispense social or humanitarian services to vulnerable populations in an effort to radicalize communities and build local support. In many cases, these organizations are fraudulent or sham charitable organizations; they are established with purported charitable aims, but operate almost solely to facilitate TF or support for a terrorist group. For example, Abdallah Faysal Sadiq al-Ahdal was designated on December 7, 2016, pursuant to E.O. 13224, for providing financial and material support to or in support of AQAP as well as acting for or on behalf of AQAP.[101] Among other support he provided to AQAP, al-Ahdal controlled the Yemen-based Rahman Charitable Organization (RCO), which he established to raise and move funds on behalf of AQAP.[102] Treasury also designated the RCO, pursuant to E.O. 13224 for being controlled by al-Ahdal.

Similarly, Treasury designated James Alexander McLintock and the Al-Rahmah Welfare Organization (RWO) pursuant to E.O. 13224 on March 31, 2016 for providing financial, material, or technological support for, or financial and other services to or in support of, AQ, the Taliban, and LeT.[103] McLintock served as the president, CEO, and chairman of the Pakistan-

[101] Treasury, Press Release, "Treasury Designates Key Facilitators and Front Company Providing Support to Al-Qa'ida in the Arabian Peninsula," Dec. 7, 2016. Available, at https://www.treasury.gov/press-center/press-releases/Pages/jl0673.aspx.
[102] *Id*.
[103] Treasury, Press Release, "U.S. and Saudi Arabia Designate Terrorist Fundraising and Support Networks," Mar. 31, 2016. Available at https://www.treasury.gov/press-center/press-releases/Pages/jl0400.aspx.

based RWO—a front organization for AQ that has been used to finance al-Qaida, the Taliban, LeT, and other Afghan extremist groups.[104] McLintock used RWO to solicit hundreds of thousands of dollars from unknowing donors, including in the UK and Persian Gulf, under the false pretense of helping Afghan orphans, but actually funneled these donations to support AQ and the Taliban.[105] Additionally, on May 11, 2017, Treasury designated Pakistan-based Welfare and Development Organization (WDO) for being controlled by a leader of Jamaat ud-Dawa al-Quran (JDQ). WDO ostensibly collected money for charity and facilitated the transfer of funds from the Gulf countries to Afghan insurgents.[106] Terrorist groups have also used religious schools to raise and transfer funds for militant activities. On March 31, 2016, the U.S. and Saudi Arabia jointly designated Pakistan-based Jamia Asariya Madrassa and its head, Abdul Aziz Nuristani, in part for facilitating financial support from Gulf-based donors to LeT.[107]

U.S. persons seeking to join ISIS have also sought to use charitable causes or association with charitable organization as a cover for their travel to conflict zones. In one case, two individuals sentenced in July 2016 for trying to travel from the United States to Syria and serve as FTFs discussed how using the cover of a charity would make it easier to get into Syria, and that if questioned about their travel by officials, could assert they were traveling for charitable reasons.[108]

As the U.S. government identifies and disrupts terrorist support networks, including those that misuse charitable organizations abroad, terrorist groups adapt to these actions. Terrorist supporters may change the name of their charitable organization or form a new charitable organization, including where the new organization has many of the same directors or officers as the prior charitable organization subject to enforcement activity.

For example, on April 7, 2015, the U.S. and the Kingdom of Saudi Arabia jointly took action to disrupt the financing and operations of Al-Furqan Foundation Welfare Trust, which is the successor entity to the Afghan Support Committee (ASC) and Revival of Islamic Heritage Society (RIHS) branches in Pakistan and Afghanistan (RIHS-Pakistan). Both were designated as SDGTs and listed on the UN ISIL and AQ Sanctions List in 2002.[109] The U.S. updated the existing designation of ASC and RIHS-Pakistan because they are a single organization that changed its name to Al-Furqan Foundation Welfare Trust in order to continue its TF activities. In March 2016, the U.S. identified Pakistan-based East and West Enterprises as another alias used by ASC and RIHS-Pakistan.[110]

---

[104] *Id*.
[105] *Id*.
[106] Treasury, Press Release, "Treasury Targets Pakistan-Based Terrorist Leaders and Facilitators," May 11, 2017. Available at https://www.treasury.gov/press-center/press-releases/Pages/sm0080.aspx.
[107] Treasury, Press Release, "United States and Saudi Arabia Designate Terrorist Fundraising and Support Networks" Mar. 31, 2016.
[108] DOJ, Press Release, "Raleigh men sentenced for conspiracy to provide material support to terrorist," July 5, 2016. Available at https://www.justice.gov/usao-ednc/pr/raleigh-men-sentenced-conspiracy-provide-material-support-terrorist.
[109] Treasury, Press Release, "The U.S. and Saudi Arabia Take Joint Action Against Terrorist Financing Entity Attempting to Evade U.S. and UN Sanctions and Violate Saudi Laws," April 7, 2015. Available athttps://www.treasury.gov/press-center/press-releases/Pages/jl10019.aspx.
[110] Treasury, Counterterrorism Designations Update, March 31, 2016. Available at https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20160322.aspx.

In the United States, terrorist groups and their supporters also raise funds under the false pretenses of charity (claiming the funds are for a charitable cause), even though the fundraiser is not necessarily affiliated with a tax-exempt charitable organization.

F. VIRTUAL CURRENCY

Virtual currencies, such as bitcoin and other decentralized convertible virtual currencies, along with other emerging payments technologies, present potential benefits for consumers and the speed and cost of financial services, but may be vulnerable to abuse by terrorist financiers because they enable potentially anonymous cross-border person-to-person funds transfers.[111] Some terrorist supporters view virtual currency as a possible mechanism to move funds globally and avoid detection by law enforcement.

Since 2015, U.S. authorities have identified a limited number of instances of terrorist groups and their financial supporters seeking donations in virtual currencies (primarily bitcoin), as well as some isolated examples of terrorists' using virtual currencies (primarily bitcoin) to move funds or pay for limited types of goods or services. However, according to information available to the U.S. government, the vast majority of terrorist funds raised in the United States still move through banks, money transmitters, and cash.[112]

A few terrorists groups, primarily ISIS and its regional affiliates, have solicited bitcoin donations from supporters. For example, ISIS supporters in the United States and abroad have sought donations in bitcoin to fund cyberattacks and other ISIS activities.[113] In one case, an ISIS supporter in the United States posted an online tutorial explaining how to fund ISIS using bitcoin.[114] The Mudjahidin Shura Council in the Environs of Jerusalem, a group supporting ISIS, also solicited funds in bitcoin to support its terrorist activities.[115]

U.S. authorities have identified a few instances where terrorists or their supporters have allegedly transacted in virtual currencies (primarily bitcoin) to support terrorist activity. For example, on December 14, 2017, U.S. authorities charged an individual with bank fraud and money laundering for defrauding numerous financial institutions of over $85,000.[116] The defendant allegedly purchased bitcoin and other virtual currencies in an attempt to "layer" the illicit proceeds before converting the funds to U.S. dollars and transferring those funds to a bank account in her name, then ultimately wiring the funds to individuals and apparent shell entities in

---

[111] FATF, Guidance for a Risk-Based Approach to Virtual Currencies, June 2014.
[112] Between January 2015 and February 2017, FinCEN identified 22 BSA reports linking bitcoin to terrorism. Over this same period, FinCEN received over 4,000 SARs flagged for TF, 90 percent of which were filed by banks and MSBs, and U.S. authorities alone arrested dozens of individuals for providing material support to ISIS and other terrorist groups.
[113] DOJ, Press Release, "Virginia Teen Pleads Guilty to Providing Material Support to ISIL," June 11, 2015. Available at https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.
[114] *Id*.
[115] European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses* at 29, May 2018. Available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.
[116] DOJ, Press Release, "Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists," Dec. 14, 2017.

Pakistan, China and Turkey.[117] In at least two other cases, U.S. individuals who were not affiliated with ISIS but allegedly either sought to conduct a terrorist attack or travel abroad to join ISIS accessed bitcoin accounts to help pay for expenses associated with their activity.[118] In another case, the registered owner of websites featuring ISIS propaganda allegedly received and made bitcoin payments to service providers.[119] In a few other examples, confirmed or suspected terrorists and their supporters established bitcoin accounts and conducted transactions, but the connection between their bitcoin use and terrorist activity is unclear.[120] These groups may view Bitcoin and other virtual currencies as an efficient way to transfer funds without detection by financial institutions or law enforcement.

While these cases indicate that some terrorist groups, terrorists and their supporters are seeking to use, and have used bitcoin for transactional activity, Bitcoin and other virtual currencies do not currently pose a significant TF risk. This assessment is based on the limited scale of virtual currency payments and funds transfer activity, as well as other factors. For instance, in some of the identified cases involving Bitcoin, it does not appear that virtual currency was used for the purpose of anonymizing transactional activity, since a more conventional payment instrument (also subject to existing AML program requirements) was ultimately used to complete the transaction.[121] Virtual currencies' utility to terrorists is also limited because it is not widely accepted as a means of payment and can be used to pay for only a limited set of goods and services. Additionally, several of the cases of Bitcoin use involved individuals who were not identified as key operatives, financial facilitators, or supporters of a particular terrorist group. It is unclear whether senior terrorist financial officials are willing to adopt new payment technologies, such as virtual currencies.

Although terrorist use of virtual currencies to move funds does not currently present a significant TF risk, several factors may cause this assessment to change. If virtual currencies become more commonly used across the globe (especially in areas that currently have poor financial and telecommunications infrastructures) and are more widely accepted to pay for goods and services from merchants and other providers, terrorist organizations, terrorists, and their supporters may become more comfortable with using it as a medium of exchange. Additionally, U.S. authorities' efforts to identify and mitigate the TF risk associated with virtual currencies have benefited from the application of U.S. AML/CFT requirements, including SAR filing obligations, to virtual currency exchangers and administrators.[122] However, most countries have yet to subject virtual currency exchangers and administrators to AML/CFT regulation. Accordingly, TF activity involving virtual currencies may be occurring without detection.

---

[117] *Id*.
[118] Information derived from an analysis of financial institution reporting.
[119] *Id*.
[120] *Id*.
[121] In the case of Zoobia Shahnaz, while bitcoin was used at an intermediate stage to disguise the origin of the funds, the funds were converted back into fiat currency, deposited into her personal checking account, and wired abroad.
[122] See FinCEN, Guidance, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013.

CONCLUSION

The wealth and resources of the United States continue to make it an attractive target for terrorist financiers raising funds to support activity outside of the United States, and the central role played by U.S. financial institutions in processing global payments expose the U.S. financial system to risk from transferring funds that are ultimately being sent on behalf of terrorist organizations or their supporters.

Multiple terrorist groups, including ISIS and its regional affiliates, AQ and its regional affiliates, Hizballah, ANF, and Al-Shabaab, benefit from funds provided by U.S.-based individuals. These groups and their supporters target certain diaspora communities and aggressively use social media to identify followers and solicit financial or other forms of material support, such as traveling abroad to serve as FTFs. U.S.-based supporters of these groups also raise funds from legitimate commercial activity and from criminal activity, and may also procure commercial goods from U.S. companies.

Despite the considerable mitigation measures and efforts of U.S. banks, the U.S. banking system is exposed to TF risk, such as from foreign respondent banks that may not have effective AML/CFT programs. TF facilitators may seek to abuse MSBs to move funds through the banking system, and while financial regulatory, supervisory and outreach efforts have mitigated much of the potential vulnerability, risk remains, especially from complicit MSB employees assisting TF facilitators. The U.S. government has also aggressively prosecuted persons or entities operating as unlicensed money transmitters and worked with financial institutions to develop measures to more effectively recognize such activity; however, given the difficulty in identifying these transactions and their observed use to facilitate TF, some risk does remain. Terrorist groups who place a priority on operational security will also seek to use U.S. currency to move funds, despite the increased cost and time for moving cash.

Overall, the U.S. charitable sector has been significantly strengthened against TF abuse through both government actions and charities' efforts at enhancing transparency, due diligence and risk mitigation. Those U.S. charitable organizations that operate or send funds abroad or that have branches outside of the United States, particularly in high-risk areas where ISIS, AQ, and other terrorist groups are most active, such as Afghanistan, Pakistan, Somalia, Syria, and Yemen, continue to face potentially higher risk of TF abuse, while those U.S. charities operating solely domestically face low TF risk, which are the vast majority of U.S. charities.

While there have been some instances of terrorist groups soliciting funds in virtual currencies such as bitcoin, and using virtual currencies to move funds or purchase goods or serves, virtual currencies do not currently present a significant terrorist financing risk. However, inadequate regulation and supervision in most jurisdictions worldwide exacerbates the money laundering, terrorist financing, and sanctions evasions risks that virtual currency payments present. To address these challenges, the U.S. government has developed a comprehensive and coordinated approach to dismantle terrorist financial networks in the United States and overseas.

Through the targeted and complementary use of law enforcement authorities, financial sanctions, and other financial tools, the U.S. has been able to identify and disrupt the actions of terrorist

financiers and other terrorist supporters, including investigations, prosecutions and financial sanctions targeting ISIS, AQ and Hizballah financiers and facilitators. ISIS leaders and operatives have been aggressively targeted around the world, resulting in the U.S. sanctioning fifteen ISIS branches along with more than 95 ISIS senior leaders, operatives, financial facilitators, recruiters, and affiliated MSBs since 2014. U.S. efforts to disrupt ISIS financing have gone well beyond financial sanctions to include targeted air strikes against ISIS cash storage sites and support for regulatory and enforcement action by the Iraqi government.

The U.S. government has aggressively utilized financial tools to limit AQ funding streams globally. This includes designating over 160 individuals affiliated with AQ and other terrorist organizations throughout Afghanistan and Pakistan, over 70 individuals and entities across the Gulf, and several more in Africa and other countries. U.S. authorities have used financial sanctions to designate Hizballah supporters in over 20 countries, including in the Western Hemisphere, West Africa, and across the Middle East, including designations of over 25 Hizballah-affiliated individuals and entities in 2018 alone– more than any previous year.

Along with the use of financial sanctions, U.S. law enforcement, led by the DOJ, has disrupted numerous avenues of support for terrorists and terrorist organizations through the investigation and prosecution of dozens of individuals in the U.S. and abroad for providing material support to designated foreign terrorist organizations.

The U.S. amplified these efforts by sharing information and collaborating with foreign partners to support their own targeted action, both bilaterally and through innovative mechanisms such as the Terrorist Financing Targeting Center. Working through the Terrorist Financing Targeting Center, the U.S. and its Gulf partners have issued coordinated designations targeting ISIS, AQ, the Taliban, and Hizballah.

These targeted measures are also built upon a foundation of financial transparency that prevents terrorist from anonymously raising, moving, and using funds, including through the development and effective implementation of international AML/CFT standards and by continuing to share information and engage with our private sector partners, both financial institutions and charitable organizations. Through these systemic efforts, the U.S. has been able to close off gaps in the U.S. and international financial system that terrorist groups can exploit and provide our partners and allies with tools, information and authorities that can be used to identify, report, and take action against terrorist financing.