ACAMS

Anti-Financial Crime Briefing

2022 National Terrorist Financing Risk Assessment

Summary

The U.S. Treasury Department released the **2022 National Terrorist Financing Risk Assessment (NTFRA)** on March 1, 2022. The risk assessment focused on the Islamic State, Al Qaida, Hizballah, and domestic violent extremists (DVEs). To determine risk, the analysts looked at threat, vulnerabilities, and consequences from the terrorist organizations. The listed groups were noted to be the most active in raising or moving funds through the United States financial system. The greatest threat to the homeland was listed as "US based individuals acting alone, reliant on their personal finances and exploiting social media to hide their radicalization". Terrorism remains a "significant concern" to the United States.

Key Takeaways

- Financial institutions in the United States have robust anti-money laundering (AML)/ counter-terrorist financing (CTF) protocols, however as technology evolves, terrorist groups can exploit vulnerabilities posed by increasing anonymity on the internet.
- The Islamic State, Al Qaida, and Hizballah remain top threats to the US financial system and the safety of the United States.
- Domestic violent extremism poses a new, serious risk to the people of the United States and its financial institutions. However, as they are widely self-funded and have no inherent terrorist financing (TF) red flags, the typologies and red flags linked to TF need to be modernized to include DVE risks and vulnerabilities in technology.
- Banks and money service businesses (MSBs) remain the main institutions terrorists use, although the risk associated with virtual currencies is increasing as their use becomes more widespread.
- Cash and the misuse of charitable organizations continue to be exploited by terrorist organizations for funding.

Differences from the 2018 Report

- In the 2022 report, there is an emphasis on domestic terrorist groups, which were not mentioned previously.
- The Taliban was not listed in the 2022 report, but was included in 2018 and in previous reports.
- In the 2022 report, Africa was noted but not focused upon.
- In 2018, virtual currencies were concluded to not be a TF risk.
- In 2018, the most common TF risk from the US was individual supporters knowingly providing funds to terrorist organizations.
- COVID-19 impacted cyberactivity, including new payment technology.
- New technology is vulnerable to exploitation and increased anonymity.
- A leading source of revenue for terrorist organizations is proceeds from criminal activity.

US Financial System Vulnerabilities

It can be difficult to distinguish terrorist financing from licit financial flows. As a result, it is imperative to increase public-private partnership, and share intelligence between law enforcement and banks regarding suspicious activity and suspicious individuals.

Banks

Banks are the primary channel of movement of terrorist funds, as large amounts of funds are moved daily, globally, making it easier for transactions to blend in. Terrorist organizations (TOs) are familiar with AML/CTF controls and continue to circumvent the systems and exploit weaknesses abroad. Sympathizers are often willing to execute transactions on behalf of TOs in intermediary countries to avoid detection. Correspondent banking can also be exploited by employees who are sympathizers. The most flagged transactions in suspicious activity reports (SARs) are "outbound transfers from US persons attempting to provide funds for groups abroad". As the transactions are often in low dollar amounts and may not raise any red flags, it is important for law enforcement to share suspicious individuals so banks can flag individuals.

Money service businesses

MSBs are often preferred for illicit activity and terrorist financing due to anonymity, speed, and efficiency. Some MSBs do not verify identification, and they often have lax AML/CFT controls abroad. They also operate near conflict zones, unlike most banks, and are vital for humanitarian needs around those areas. Complicit employees have been known to move terrorist funds by operating as an agent, especially regarding Al Qaida. MSBs are commonly used by foreign terrorist fighters seeking to join TOs and to transfer funds overseas.

Unlicensed money transmitters

Unlicensed money transmitters, such as in businesses like grocery stores and gas stations, have been identified in terrorist financing. They may facilitate transactions like exchange houses, and transfer funds on behalf of terrorist organizations or individuals. Cash is also a preferred method for TOs; it allows for anonymity, does not leave a trail, and can be smuggled across borders.

Virtual assets

The TF risk from virtual assets has increased since 2018. Virtual assets often allow for anonymity while enabling peer-to-peer cross-border fund transfers instantaneously. This aligns with the increased use of social media recruitment and donation mechanisms. However, virtual assets can be difficult to use for TOs in conflict zones and in areas with poor telecommunication infrastructure. TOs often need fiat currency and virtual asset kiosks are generally not set up in conflict areas.

Charities

Charities have been exploited by TOs in the past and continue to be exploited presently. Funds can be directed to TOs, or charities may assist in logistics and recruitment for TOs. In addition, terrorists have set up front charities to move funds through the international banking system. Some charities are at a higher risk of exploitation due to their geographical location and activities. US based charities often go through vetting processes but may be at risk from local contractors. The Islamic State also uses the refugee camp in Syria, al-Hawl, to raise funds through humanitarian appeals from foreign supporters.

Listed Terrorist Organizations

	Islamic State	Al Qaida	Hizballah	DVEs
Threat to US	Remains capable of – and committed to – attacking the US	Severe leadership losses, but continues to encourage US attacks	Maintains capability to target US interests abroad	Currently the most urgent threat to US national security
Coordination	Central financial system that funds core network and redistributes to cells based on needs and priorities	Cooperation among decentralized cells globally	Established international financing and procurement network globally with front import/export companies	Often individuals or small cells radicalized online by larger organizations
Fundraising	Kidnapping for ransom, looting, extortion, donations, gold mining, virtual assets, cash reserves from oil or taxation	Licit business activities, front charities, virtual assets, donations; some cells in areas with weak governance use taxation, permit fees	Main source of support is from Iran, also criminal activity (drug and arms trafficking)	Self-financing, crowd sourcing (chatrooms, social media), donations, membership fees, commercial activities (merchandise and events)
Expenditures	Fighter salaries and payments to imprisoned or deceased fighters' families	Not listed	Not listed	Property for paramilitary training, arms, tactical gear
US-Based Financing	Individual supporters use personal savings or collect donations to travel, fund travel, or transfer funds abroad	Funds sent by individual supporters or through front charities to support organization	Funds will enter the US banking system though comingling legal and illegal commerce; supporters sending money into the US	Occurs domestically, becoming increasingly transnational
Money Movement	Moves money through shell companies, complicit individuals, or operatives in non-conflict zones	Uses financial facilitators to move money to conflict zones	Complex TBML schemes, exploiting free trade zones, weakly regulated banks, money exchanges, and unregulated networks	Normal and licit activity, no identifiable tie to terrorism, not in a high-risk jurisdiction; often personal savings accounts or peer-to-peer transactions

Financial Institution Considerations

Financial institutions, including money service businesses, play an essential role in combatting the financing of terrorism. It is imperative that financial institutions follow the money trail and understand how these terrorist organizations operate, their motives and beliefs, and how they manage their finances. Understanding these components will allow for more effective detection and reporting of terrorist financing activity.

Financial institutions should consider the following reports alongside the 2022 National Terrorism Risk Assessment:

- **FinCEN Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies** (FIN-2021-A003), March 2021
- **FATF Report: Ethnically or Racially Motivated Terrorism Financing,** June 2021
- **FinCEN's US National Priorities,** June 2021

Within their organizations, financial institutions should consider taking the following action:

- Identify TF risks within both your AFC and sanctions compliance programs. Remember, as stated in the report, the risk is a function of threat, vulnerability, and consequence. Financial institutions should assess their risk in consideration of their products, services, customer base, and geographies served. Based on those risks, AFC programs, including KYC/CDD/EDD, transaction monitoring rules and typologies, investigation standards, and expertise and resources, including human capital and technology, should be shifted, and aligned to those risks.
- As required under 31 CFR § 1010.610(a), ensure that your due diligence programs, which address correspondent accounts maintained for future financial intelligence sharing, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls. These should be reasonably designed to detect and report known, or suspected, money laundering activity, conducted through or involving any correspondent account established, maintained, administered, or managed in the United States.[1]
- When filing a SAR for an activity involving a jurisdiction identified in the FinCEN FIN-2021-A003 Advisory, at the request of FinCEN, you should reference this advisory in SAR Field 2 (Filing Institution Note to FinCEN) and the narrative, by including the following key term: "FATF FIN-2021-A003".[2]
- If you suspect terrorist financing activity and file a SAR, it is recommended that you check box 33(a) or 33(z) on the SAR form and include all pertinent available information in the SAR form and narrative. Additionally, you should call the FinCEN financial institutions toll-free hotline at (866) 556-3974.[3]

1. FinCEN, March 11, 2021, FinCEN Advisory FIN-2021-A003, **https://www.fincen.gov/sites/default/files/advisory/2021-03-11/FATF%20February%202021%20Advisory%20FINAL%20508.pdf**
2. FinCEN, March 11, 2021, op. cit.
3. FinCEN, March 11, 2021, op. cit.

- Enhance your AFC training program to include TF risks and tailor the training to the appropriate audience. Training should consist of current red flag indicators, and typologies tied to terrorist financing activity risks identified in the institution. In addition, front-line tellers should have tailored training on potential TF or terrorist red flags tied to KYC, CDD, and transactions that may involve jurisdictions of high risk.

Conclusion: Areas for Consideration

Public-private partnership

The 2022 report listed that public-private partnership was vital to monitoring terrorist financing risks; however, it appears there was no private sector input incorporated into the report. The U.S. Treasury Department should consider convening a supervisory team of relevant private sector experts from financial institutions, crypto firms, cyber intelligence firms, and SMEs in vulnerable and unregulated industries to understand the threats, risks, and vulnerabilities that exist outside of the regulatory filings. The private sector intelligence and information gained could be incorporated into both the National Risk Assessments and the US strategy to combat terrorist and other illicit financing.

Emerging technologies

The risk assessment identified an increased risk from emerging technologies and virtual currencies. The industry, specifically financial institutions and money service businesses, would benefit from a government issued report identifying the current red flags, typologies, and mechanisms in which these emerging technologies and virtual currencies are being exploited. This would allow industry to update their AFC programs accordingly, resulting in more effective detection and reporting to FinCEN.

The industry approach of "left of boom"

The AML/CTF typologies and red flags should be updated regularly and proactively, to stay ahead of vulnerabilities within emerging technology and the US financial system to effectively combat terrorist financing risk. This could be accomplished through increased information sharing and enhanced public-private partnership.

Authors

Lauren Kohr, Senior Director, AML – Americas
Tiffany Polyak, CAMS, Project Coordinator/Researcher

March, 2022

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60 Chapters globally further amplify the association's mission through training and networking initiatives. Visit **acams.org** for more information.