Identifying and Preventing Terrorist and Other Illicit Financing

Terrorists and terrorist groups and other criminal actors engage in a variety of financial schemes (see figure) to raise, move, store, and spend large amounts of illegally gained money. Some of these schemes include theft, fraud, identity theft, tax evasion, counterfeiting, and money laundering, with some terrorists and other criminals using increasingly sophisticated techniques.

SCOPE: This product is the first in a series of assessments on illicit finance–related topics. It identifies indicators and provides resources for public and private sector partners investigating terrorism-related financial crimes.

Terrorists and other criminals acquire illicit income through several means, including the abuse of legitimate sources like charities, schools, crowdfunding, membership fees, and legal business ventures such as concerts, sporting events, and merchandise sales; state sponsors; and criminal activities such as kidnap-for-ransom operations and extortion. Two examples provided below demonstrate the intent of terrorists to illicitly fund their activities.

- In June 2022, the Department of the Treasury Office of Foreign Asset Control identified two key supporters of the Russian Imperial Movement (RIM), a racially or ethnically motivated violent extremist group that espouses the superiority of the white race.[*] RIM sought to raise and move funds with the intent of building a global network of violent extremist groups, including fundraising to purchase weapons and military equipment in support of pro-Russian separatist fighters. The Department of State designated the group as a specially designated global terrorist (SDGT) organization in April 2020 for providing terrorism training.
- In August 2020, the Department of Justice announced a series of forfeiture actions to dismantle several cyber-enabled terror finance campaigns supporting ISIS, al-Qa'ida, and HAMAS. Authorities seized millions of dollars, more than 300 cryptocurrency accounts, four websites, and four social media accounts related to the criminal enterprise.

Figure: Financial Schemes of Terrorist Groups

[*] Racially or ethnically motivated violent extremists (RMVEs) have ideological agendas that derive from bias—often related to race or ethnicity—held by the actor against others, including a given population group.

16573-NCTC

5 December 2022
Authored by NCTC, DHS, FBI

The ISIS-related criminal complaint highlighted an alleged scheme by an ISIS facilitator responsible for managing cyber hacking operations who was involved in selling fake personal protective equipment. Site administrators claimed access to unlimited supplies of N95 respirator masks in spite of such items being officially designated as scarce. These items were available for purchase to customers across the globe, including a customer in the United States who sought to purchase N95 masks and other protective equipment for hospitals, nursing homes, and fire departments.

INDICATORS: Public and private sector partner awareness of financial crime helps identify an array of potential financial crime threats tied to money laundering and other illicit financing activity in support of terrorism. In addition, awareness of indicators associated with illicit financial activities can enhance detection, prevention, collection, and mitigation. Although a single indicator may not be suspicious, two or more indicators may signify suspicious activity based on the totality of circumstances. Among such indicators that would raise suspicion in a reasonable person and may warrant further investigative action including the following:

- Cash deposits in different banks within a short time frame, especially when quickly followed by withdrawals or transfers out
- Cash deposited locally with the funds subsequently withdrawn from other locations—which could be inside or outside the United States—that are not known to be frequented by the investigative subject
- Frequent early repayment of loans, especially with cash
- Frequent overpayment of multiple credit cards, followed by cash-advance withdrawals
- Bank drafts cashed in for foreign currency
- Frequent gambling activity with low returns but higher chances of winning or large amounts of chips purchased and cashed in with little or no gambling activity
- Large amounts of cash from unexplained sources or deposits or other financial activity inconsistent with known (or claimed) sources of income
- Large cash deposits used for investment or deposited into company accounts
- Purchase of high-value assets such as cars, jewelry, and property with cash, especially if resold quickly
- High trade volume between different types of cryptocurrencies

CONSIDERATIONS: To avoid detection by authorities, terrorists use evolving illicit financial tactics, techniques, and procedures (TTPs). Awareness of current TTPs as well as the current threat landscape can help public safety officials identify violent extremist connections and improve their abilities to respond to and mitigate threats.

Support from senior and executive leadership is critical to ensuring that authorities prioritize counterthreat finance throughout the investigative process. Participation in financial crime training and multidisciplinary exercises are also key to increase collaboration across the public and private sector.

Collaboration: Partnerships with subject matter experts can assist with the technical requirements of terrorism-related financial crimes investigations. The following are recommendations to help first responders and their organizations identify indicators of potential financial crimes and available tools and resources to help investigations.

- Partner with federal agencies with expertise in financial crime investigations, including the FBI, Internal Revenue Service (IRS), and the DHS/Homeland Security Investigations (HSI). Outreach with state and local partners can provide access to information that may be pertinent to illicit financial investigations, including tax and property records.
- Leverage private sector partners with expertise in the financial system. Specialized knowledge from and financial networking with banks and money service businesses, blockchain[†] forensics experts, and financial technology firms may provide beneficial resources during investigations, including investigations that involve cryptocurrency transactions.
- Understand indicators of suspicious financial activity. For private sector partners, increasing financial institutions' awareness of indicators of suspicious financial activity can lead to enhanced suspicious activity reporting.
- Share information and network with subject matter experts. State and local fusion centers and the FBI's field offices and joint terrorism task forces (JTTFs) are valuable resources to share information and network with subject matter experts who have insights into financial schemes, to include TTPs.

[†] Blockchain is a decentralized public ledger organized into a series of chronological, interlinked data blocks. Cryptocurrencies rely on these blockchains to facilitate transactions, and, in some cases, blockchains can perform other functions not related to currency transactions.

Federal Government Roles in Fighting Illicit Finance

A range of federal agencies support the disruption, prevention, investigation, prosecution, and recovery of illicit terrorist and criminal financial proceeds across the interagency. Partnerships across a diverse range of organizations can assist in detection, investigative, and potential mitigation efforts.

- **Department of the Treasury:** Treasury's Office of Terrorism and Financial Intelligence identifies, disrupts, and dismantles threats to, and identifies and reduces vulnerabilities in, the United States and international financial systems to prevent abuse by illicit actors.
- **Department of Justice:** The National Security Division, Money Laundering and Asset Recovery section, US Attorney Offices, FBI, DEA, and other investigative and prosecution components and agencies use a wide variety of resources and subject matter expertise to disrupt illicit activity and enforce US laws.
- **DHS:** Immigration and Customs Enforcement (ICE) and HSI are positioned to disrupt the operations of transnational criminal organizations profiting from cross-border crime. HSI conducts financial investigations to identify and seize illicit proceeds and to target financial networks that launder and hide illicit funds. The Secret Service's primary investigative mission is to protect the financial infrastructure of the United States by investigating complex, often cyber-enabled, financial crimes.
- **Department of State:** State pursues diplomatic solutions to proliferation challenges, terrorism, and other transnational criminal activities and maintains the ability to impose certain financial and economic sanctions through the designation of foreign terrorist organizations, state sponsors of terrorism, and SDGTs.
- **Department of Defense:** Dedicated counterthreat finance teams within the DOD analyze financial intelligence, integrate intelligence and operations, and coordinate and execute counterthreat finance efforts at each of the geographic combatant commands, US Special Operations Command, US Transportation Command, and the National Guard Bureau.
- **Supervisory Authorities:** Federal functional regulators—including the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Securities and Exchange Commission—supervise, examine, and enforce compliance with anti–money laundering and terror financing laws and regulations.

Training:[‡] Incorporating an array of threat scenarios in multidiscipline exercises—including illicit financial activities—can help identify response capabilities and mitigation strategies. Increased familiarity of partner capabilities, authorities, and policies and procedures through collaborative and cooperative environments provides opportunities to enhance incident and investigative response.

- Federal agencies such as DHS, FBI, and IRS frequently provide access to training courses for state, local, tribal, and territorial (SLTT) investigators. For example, Federal Law Enforcement Training Centers (FLETC) courses include the following: the Money Laundering and Asset

[‡] NCTC lists these materials and trainings to illustrate the variety of offerings and does not endorse the content of the material or trainings these organizations offer.

Forfeiture Training Program, Financial Investigations and Analysis Training Program, and International Banking and Money Laundering Training Program.

- The National White Collar Crime Center (NW3C)—a private sector, not-for-profit organization—sponsors in-person and online training relevant to SLTT financial crime investigators and analysts. NW3C courses include the following: Overview of White Collar Crime, The Bank Secrecy Act, Virtual Currency, and Combating Transnational Crime and Terrorism Financing.

RESOURCES:

DHS

- **Science and Technology Directorate—Anonymous Networks and Currencies** provides solutions for law enforcement to assist with criminal investigations using anonymous networks and currencies. https://www.dhs.gov/science-and-technology/anc
- **State and Major Urban Fusion Centers** empower frontline law enforcement, public safety, fire service, emergency response, public health, and private sector security personnel to lawfully gather and share threat-related information. https://www.dhs.gov/fusion-center-locations-and-contact-information
- **Secret Service—National Computer Forensics Institute** offers training to SLTT partners in cryptocurrency investigations as well as cyber and emerging technologies. www.NCFI.usss.gov
- **ICE, HSI—National Bulk Cash Smuggling Center–Crypto Intelligence Program** provides operational support to federal, state, local, and international agencies involved in the enforcement and interdiction of bulk value and illicit proceeds moved through various methods. BCSC@ice.dhs.gov; Tipline: 866-DHS-2-ICE; https://www.ice.gov/webform/ice-tip-form
- **FLETC** provides a wide range of training to law enforcement officials, including financial topics. https://www.fletc.gov/training-catalog
- The **Public-Private Analytic Exchange Program** is a joint analytic partnership between private-sector partners and US Government analysts and seeks to promote greater understanding of a range of national security and homeland security issues. Topic teams publish unclassified analytic deliverables for government and private sector and are available to the public. https://www.dhs.gov/aep-deliverables
    - Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies (2022)
    - Blockchain and Suitability for Government Applications (2018)

FBI

- **JTTFs** are cells of highly trained, locally based investigators and analysts from dozens of US law enforcement and intelligence agencies. www.fbi.gov/contact-us/field-offices
- The **Money Laundering, Forfeiture, and Bank Fraud Unit (MLFBU)** is responsible for supporting all cases with a money laundering nexus. MLFBU works across the interagency to pursue complex, multidistrict and international money laundering and asset forfeiture investigations. 1-800-CALL-FBI; https://www.fbi/gov/contact-us

The **FEDERAL TRADE COMMISSION** seeks effective law enforcement against deceptive, unfair, and anticompetitive business practices, creates and shares educational programs; advances consumers' interests; and develops policy and research tools. https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams#paying; ReportFraud.ftc.gov

The **FINANCIAL CRIMES ENFORCEMENT NETWORK** provides support and resources to law enforcement to assist with investigations and provides training opportunities related to financial crimes. www.fincen.gov

INTERPOL provides the findings on criminal finances and cryptocurrencies from an international conference it hosted with Europol and the Basel Institute on Governance in December 2021. The findings were intended to inform law enforcement, regulators, and private sector officials about broad approaches to protect citizens and the global economy from illicit activity. https://baselgovernance.org/sites/default/files/2022-01/2021%20Recommendations%20Crypto%20AML.pdf

The **NW3C** supports law enforcement and regulatory agencies involved in prevention, investigation, and prosecution of economic and high-tech crimes through training opportunities. https://www.nw3c.org/online-training-selection

- **Bitcoin Investigative Field Guide** provides information regarding commonly asked questions that law enforcement officers may have when dealing with cryptocurrency-related investigations specific to Bitcoin. www.nw3c.org/resources/Bitcoin-investigative-field-guide/Bitcoin-IFG.pdf

The **DEPARTMENT OF JUSTICE CRYPTOCURRENCY ENFORCEMENT FRAMEWORK** highlights how malicious actors use and misuse cryptocurrency to facilitate illegal activities and identifies key legal authorities and partnerships to combat threats to national security as well as approaches to address growing public safety challenges. https://www.justice.gov/archives/ag/page/1326061/download

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

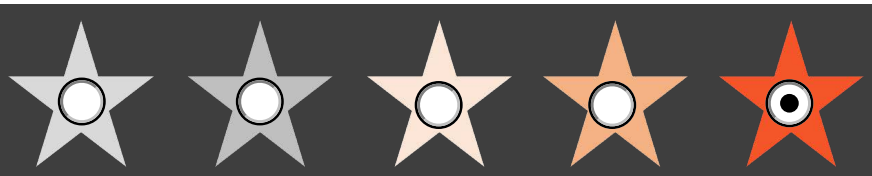
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: Identifying and Preventing Terrorist and Other Illicit Financing

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT