Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated November 27, 2023

Terrorist Financing: Hamas and Cryptocurrency Fundraising

Policymakers, including some Members of Congress, are scrutinizing U.S. efforts to counter the role that cryptocurrency fundraising plays in the financing of terrorism. A key question for Congress is whether further regulation of the virtual asset sector and/or the introduction of additional countermeasures are necessary to prevent terrorist financing. The issue has attracted congressional attention in the wake of the October 7, 2023, attacks on Israel perpetrated by Hamas—an Iran-supported Palestinian group identified by the United States and some others as a terrorist organization subject to sanctions. U.S. government reports indicate that Hamas has sought cryptocurrency through donation drives since at least 2019.

Role of Cryptocurrency Donations in Hamas Fundraising Campaigns

Although Hamas has reportedly solicited cryptocurrency donations, the scale and effectiveness of these efforts remain unclear. Citing two cryptocurrency analytics firms and Israeli government seizure orders, the *Wall Street Journal* reported on October 10, 2023, that cryptocurrency wallets connected to Hamas received about $41 million between 2020 and 2023 and that wallets connected to another U.S.-designated terrorist organization, the Palestine Islamic Jihad (PIJ), received as much as $93 million over a similar period. Some observers have questioned whether such figures overestimate the amount Hamas received and note the role of other, larger funding sources that sustain Hamas (e.g., the Iranian government, extortion and de facto taxation in Gaza, foreign investments, and charities).

Origins

In 2019, Hamas engaged in a cryptocurrency donation campaign that led to the U.S. seizure of several websites and 150 cryptocurrency accounts linked to the armed wing of Hamas, the Izz al Din al Qassam Brigades, in 2020. In connection with these enforcement actions, the U.S. Department of Justice (DOJ) charged two foreign nationals for money laundering crimes related to their involvement in converting cryptocurrency into other forms of value. DOJ also prosecuted an individual for concealing material support to Hamas, including through Bitcoin. U.S. enforcement actions in 2023 revealed that Qassam Brigades used Binance, a cryptocurrency exchange, to facilitate cryptocurrency transactions since as early as 2019.

Following its initial cryptocurrency campaign, Hamas's efforts to generate cryptocurrency donations continued to garner attention from prospective donors as well as law enforcement authorities. In 2021, the U.S. cryptocurrency exchange platform Coinbase identified Hamas as one of several terrorist groups involved in cryptocurrency fundraising. Israeli authorities reportedly seized dozens of cryptocurrency addresses linked to Hamas, PIJ, and other terrorist groups between 2021 and 2023. In April 2023, the Qassam Brigades announced it would stop accepting Bitcoin donations, cautioning that donors could be targeted.

Recent Developments

Since October 7, authorities appear to be on alert for signs that Hamas-linked entities may have resumed soliciting cryptocurrency donations, in order to fund the current Israel-Hamas conflict. On October 10, Israeli authorities reportedly moved to freeze additional Hamas-linked cryptocurrency accounts. For its part, the U.S. Department of the Treasury has engaged U.S. and international stakeholders in efforts to deter terrorist fundraising through cryptocurrencies. Treasury has also taken the following actions:

- Sanctioned additional Hamas operatives and financial facilitators—including a Gaza-based virtual currency exchange (Buy Cash Money and Money Transfer Company) and its operator.
- Issued an "alert" to financial institutions to counter Hamas-related terrorist financing. In the alert, Treasury's Financial Crimes Enforcement Network (FinCEN) noted the variety of ways in which Hamas raises funds, including "fundraising campaigns involving virtual currency and fictitious charities raising both fiat and virtual currency."
- Published a notice of proposed rulemaking (NPRM) that determined that transactions involving convertible virtual currency (CVC) mixing are "of primary money laundering concern" and proposed the application of enhanced recordkeeping and reporting obligations on covered financial institutions, pursuant to the first special measure outlined in Section 311 of the USA PATRIOT Act (P.L. 107-56; codified at 31 U.S.C. 5318A). (Mixers are applications that obscure the senders and recipients of cryptocurrency transactions, complicating efforts to trace funds.)
- Hosted a FinCEN Exchange to discuss threats posed by illicit cryptocurrency use in light of Hamas's attack on Israel and the role of the financial industry in countering the financing of terrorism (CFT). FinCEN encouraged financial institutions to register under the voluntary information sharing program under Section 314(b) of the USA PATRIOT Act.
- Settled with Binance over money laundering and sanctions violations (more than $4 billion in penalties), including failure to report transactions associated with the Qassam Brigades, PIJ, and other terrorist groups.

U.S. Policy Framework for CFT and Cryptocurrency Regulation

Contemporary U.S. CFT policy is grounded in anti-money laundering (AML) and counterterrorism policies that predate the advent of virtual assets and virtual asset service providers (VASPs). At issue is whether and how to modify existing AML/CFT policies and regulations to reflect the risks and opportunities posed by virtual assets.

U.S. Regulatory and Sanctions Framework for CFT

The cornerstone of U.S. AML policy originated in 1970 with the Bank Secrecy Act (BSA; P.L. 91-508) and its major component, the Currency and Foreign Transactions Reporting Act. Designations and prohibitions against state sponsors of terrorism and foreign terrorist organizations emerged in the late 1970s and evolved through the 1990s. In response to the Al Qaeda attacks on the United States on September 11, 2001 (9/11), Congress took additional CFT actions through the enactment of several public laws, including the USA PATRIOT Act and its major component, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

In response to 9/11, President George W. Bush also issued Executive Order (E.O.) 13224, which established a new counterterrorism sanctions program targeting specially designated global terrorists (SDGTs). In 2019, President Donald Trump issued E.O. 13886, amending E.O. 13224 to expand the scope of sanctionable activity and authorize secondary sanctions against foreign financial institutions that have knowingly conducted or facilitated a significant financial transaction on behalf of an SDGT. Digital currency addresses, including one related to a Hamas-linked exchange, have been sanctioned under the SDGT program.

AML/CFT Regulations for Virtual Assets

AML/CFT requirements for money services businesses (MSBs) under the BSA (finalized in a 2011 FinCEN rulemaking) generally apply to VASPs that act as money transmitters (a type of MSB). FinCEN issued guidance in 2013 and 2019 to clarify that such VASPs are required to (1) register with FinCEN as MSBs; (2) maintain an AML program; and (3) follow recordkeeping, monitoring, and transaction reporting requirements, in line with requirements for MSBs. Such reporting requirements include filing suspicious activity reports and currency transaction reports. Applicable AML/CFT requirements also include verifying customer identities and conducting related customer due diligence.

FinCEN has clarified that these requirements apply to domestic and foreign-located CVC money transmitters that do business "in substantial part within the United States," even if they are headquartered outside the United States and have no physical U.S. presence. FinCEN considers centralized and decentralized exchanges to be money transmitters subject to AML/CFT requirements. In contrast, CVC users, including those who use cryptocurrency to buy goods and services, are not considered to be money transmitters and are exempt from BSA requirements.

Congressional Outlook

Concern regarding the possibility that Hamas has benefitted from cryptocurrency donations prompted some Members of Congress to write several letters to the Biden Administration. One such letter, with more than 100 signatures, urged the Administration to "swiftly and categorically act to meaningfully curtail illicit crypto activity and protect our national security and that of our allies." In several congressional committee hearings since October 7, some Members have raised questions regarding the role of terrorist fundraising through cryptocurrencies.

Congressional attention to the terrorist financing risks posed by cryptocurrencies is ongoing amid broader debates surrounding virtual asset governance and whether the sector requires additional legislation, regulation, and supervision. Stakeholders have sought to balance the opportunities that the virtual asset sector may portend for financial sector innovation and financial inclusion with the susceptibility of virtual assets to misuse. Some observers further note that certain aspects of the virtual asset ecosystem (e.g., decentralized participants that comprise a network, such as nodes and miners) are not consistently regulated, especially internationally. Others caution against proposals for regulation that may be overly broad and ill-equipped to deal with the characteristics of the virtual asset industry and stifle innovation.

Proponents of enhanced cryptocurrency regulation may point to perceived gaps in AML/CFT compliance among VASPs, including well-known cryptocurrency exchanges (e.g., Binance and Bizlato) and mixers (e.g., Blender.io and Tornado Cash). In practice, U.S. authorities are challenged to enforce BSA requirements on foreign-headquartered transmitters, even if the exchanges conduct business with U.S. persons. FinCEN's October 2023 NPRM on CVC mixers noted that no such mixers have registered in the United States as MSBs—underscoring concerns regarding the apparent lack of AML/CFT compliance among such VASPs. Other observers may question whether regulatory changes to the cryptocurrency industry will significantly affect terrorist financing. At congressional hearings held since October 7, witnesses testified that the appeal of cryptocurrency for financing terrorist groups in particular, including Hamas, may be limited due to their susceptibility to detection by authorities (blockchain ledgers that record crypto transactions are publicly visible) and the availability of other funding sources and laundering methods.

Legislation in the 118th Congress contains provisions to address certain aspects of the virtual asset sector. For example, the two versions of a National Defense Authorization Act for Fiscal Year 2024 (NDAA; H.R. 2670 and S. 2226) would require bank supervisors and federal regulators to establish AML/CFT examination standards for financial institutions relating to crypto assets. The NDAA bills would also require Treasury to report to Congress on anonymity-enhancing services, such as mixers, and recommend policy options for preventing their use by illicit actors. Other bills have sought to address Hamas-specific illicit financing (e.g., H.R. 340, H.R. 6322, and S. 1647).

Paul Tierno, Analyst in Financial Economics
Rena S. Miller, Specialist in Financial Economics

Liana W. Rosen, Specialist in International Crime and Narcotics

IF12537

Disclaimer