November 28, 2023

**Potential Options to Strengthen Counter-Terrorist Financing Authorities**

The Treasury Department shares Congress's interest in taking immediate and decisive action on terrorist financing to disrupt Hamas's financing networks in the wake of their October 7 attack, and to help prevent future terrorist attacks. Treasury has a range of strong counter-terrorism and illicit finance tools that we have used effectively to combat terrorist financing, but modes of raising and moving money continue to evolve and many of our authorities have not been updated in decades. This creates gaps we seek to close, working with Congress. Terrorist groups including Hamas, Palestinian Islamic Jihad, ISIS, Al Qaeda and their enablers like Iran, use new virtual methods to move, store, and obfuscate their funding streams. These methods often include the use of evasive cryptocurrency networks and services, including mixers. Terrorist financiers are also adept at using third country institutions to evade and obfuscate, elevating the need for tools that empower disruption across multiple jurisdictions. Treasury has and will continue to use its existing tools effectively. Recently, for example, Treasury and its inter-agency partners assessed a $4.3 billion penalty, the largest such penalty in Treasury history, against the cryptocurrency exchange Binance, for violations of anti-money laundering and sanctions requirements. We also moved quickly after the October 7 attack to designate a Gaza-based cryptocurrency exchange used by Hamas, and issued a notice of proposed rulemaking identifying Convertible Virtual Currency Mixing (CVC mixing) as a class of transactions of primary money laundering concern, including for terror groups. However, our Bank Secrecy Act (BSA) and sanctions authorities have not kept pace with emerging payment methods, and we are committed to ensuring that our AML/CFT regime can best deter, detect, and stop illicit finance facilitated by virtual assets.

Treasury seeks to work with Congress on two high-impact efforts:

> (1) the creation of a new secondary sanctions tool that would facilitate Treasury's targeting of fintech, including cryptocurrency exchanges, that facilitate payments to Hamas and other terrorist groups; and
>
> (2) the closing of legal and regulatory gaps tied to outdated definitions and standards for financial institutions and for off-shore platforms in Treasury's BSA and International Emergency Powers Act (IEEPA)-based authorities.

These efforts will enable more focused and impactful targeting of cryptocurrency entities and services that facilitate funding for terrorists. Furthermore, the new authorities and definitions proposed would allow Treasury to do more to disrupt Hamas and their supporters' financial networks and close evasion loopholes. The proposals would require additional funding to effectively implement and supervise the covered activities. Moreover, the proposals should be augmented by increased synchronization of efforts between the Department of Commerce and the Department of Treasury, and between the Department of the Treasury and private sector institutions and associations in the cryptocurrency domain. These synchronization efforts should

focus on modernizing public/private and interagency cooperation on countering export control and sanctions evasion, including by terrorist actors.

The new authorities and definitions are proposed in more detail below.

1) ***New Secondary Sanctions Tool for Cryptocurrency Exchanges and Financial Service Providers that Facilitate Payments to Terrorist Groups***

**Legislative Proposal:** Create a statutory authorization for a new type of sanction, analogous to Correspondent Account or Payable-Through Account (CAPTA) sanctions, to deploy in the FinTech and cryptocurrency space.

**Existing Gap/Risk:** Treasury's CAPTA authorities enable Treasury to prohibit U.S. correspondent accounts and transaction processing for certain financial institutions that have operated in the financial services sectors of certain economies or facilitated transactions for a designated entity. These authorities allow for the designation of foreign financial institutions and the severing of U.S. correspondent relationships, without requiring that all property or interests in property of the designated entity be blocked, making them a powerful but tailored way to sanction financial institutions. CAPTA authorities exist across multiple sanctions programs, including Russia, counterterrorism, Iran, and North Korea programs, and have enabled disruption in banking channels of many high-priority illicit finance streams. However, unlike banks, foreign cryptocurrency exchanges and some money services businesses do not depend on correspondent accounts for all transactions. This makes some of Treasury's most powerful sanctions tools less effective at identifying and disrupting financial services provided by cryptocurrency or other FinTech companies.

In practice, we have seen certain cryptocurrency exchanges used in lieu of traditional banks to facilitate payments to terrorist groups. For example, the *Wall Street Journal* recently reported that Hamas has turned to cryptocurrency exchanges to facilitate crowdfunding. A new CAPTA-like authority aimed at virtual asset providers would allow Treasury to evolve its targeting capabilities and would account for the technological changes that have rendered highly effective tools in the traditional payments context less effective against cryptocurrencies and fund transfers by certain fintechs.

***1. Closing Loopholes in Treasury Authorities to Address Use of Cryptocurrency for Illicit Activities***

**A. Update BSA and IEEPA definitional terms.**

i. **Legislative Proposal:** Define a new cryptocurrency-related category of "financial institution" under the BSA, which includes but is not limited to cryptocurrency exchanges, Virtual Asset Service Providers (VASPs), virtual asset wallet providers, certain blockchain validator nodes, and decentralized finance services and subject it to the type of AML/CFT requirements to which banks and other financial institutions are already subject.

**Existing Gap/Risk:** Many cryptocurrency entities are considered money services businesses (MSBs) under the BSA and its implementing regulations, and many Virtual Asset Service Providers (VASPs) are required to register as MSBs if they do business in the United States. However, other cryptocurrency entities, including so-called "decentralized finance" (DeFi) platforms, have claimed that they do not meet the definition of an MSB, or that they are not subject to BSA requirements or sanctions prohibitions at all, because they lack a centralized operator or organization, or do not take custody of funds. Parts of the digital asset ecosystem, including some DeFi service providers, noncustodial wallet providers, miners, and validators are not currently subject to BSA requirements. Hamas's use of both centralized exchanges and peer-to-peer transactions between unhosted wallets is well-documented. Validator node operators themselves have also posed national security concerns. Legislation making clear that these entities are considered a type of financial institution under the BSA would help drive compliance and enable stronger enforcement.

ii. **Legislative Proposal:** Create an explicit IEEPA authority to designate blockchain nodes or other elements of cryptocurrency transactions.

**Existing Gap/Risk:** Decentralized finance activities, including, for example, the Tornado Cash mixing service, are increasingly employing "smart contract" software that purports to reside on blockchains autonomously. This poses challenges, including in the recent Tornado Cash litigation, where plaintiffs argued that the smart contracts do not constitute property or an interest in property that can be blocked by OFAC. To resolve this issue, legislation could explicitly authorize OFAC to designate particular blockchain nodes or networks, rather than requiring that they be a designated person's property or interest in property.

**B. Address jurisdictional risk from offshore cryptocurrency platforms.**

i. **Legislative proposal:** Clarify OFAC jurisdiction over USD-backed stablecoins.

**Existing Gap/Risk:** Stablecoins are cryptocurrency whose value is pegged to a reference currency such as the U.S. dollar (USD), which have become common vehicles for terrorist financing. Although OFAC would typically have jurisdiction to block transactions in USD that transit intermediary U.S. financial institutions, it does not always clearly have the same authority to block equivalent-value stablecoin transactions, because certain stablecoin transactions involve no U.S. touchpoints. Legislation could explicitly authorize OFAC to exercise extraterritorial jurisdiction over transactions in stablecoins pegged to the USD (or other dollar-denominated transactions) as they generally would over USD transactions. Such legislation would likely require an explicit statement of extraterritorial reach to accord with the Supreme Court's governing presumption against extraterritoriality. *See, e.g.*, *Abitron Austria GmbH v. Hetronic Int'l, Inc.*, 600 U.S. 412, 417 (2023).

ii. **Legislative Proposal:** Clarify that IEEPA jurisdiction extends to entities abroad with U.S. touchpoints.

**Existing Gap/Risk:** Many cryptocurrency platforms claim to be "jurisdiction-less" and structure their entities in a way to purposely evade regulatory requirements, creating issues regarding the scope of OFACs jurisdiction over foreign-based entities that do business in the U.S. IEEPA provides that OFAC may regulate or prohibit transactions "by any person, or with respect to any property, subject to the jurisdiction of the United States." However, it is often unclear to what extent OFAC may regulate transactions between foreign persons, where those transactions have some appreciable nexus to U.S. markets (as in the stablecoin example, above). Legislation could clarify that IEEPA applies with respect to conduct abroad by entities with defined U.S. touchpoints, for example, those that have established relationships with U.S. businesses operating abroad, or who serve users located in the U.S.

iii. **Legislative Proposal:** Clarify that BSA jurisdiction extends to entities abroad with U.S. touchpoints, but with option for substituted compliance for FATF-compliant jurisdictions.

**Existing Gap/Risk:** The BSA's application to entities abroad presently lacks clarity, because the BSA does not specify whether it may apply extraterritorially. By regulation, FinCEN generally defines a covered "financial institution" as "[e]ach agent, agency, branch, or office within the United States" doing business in certain capacities, and some financial institutions, like MSBs, are defined to include entities located abroad that do business "wholly or in substantial part" in the United States. However, absent a clear statutory authorization to apply the BSA extraterritorially, it is uncertain how far FinCEN's regulations could extend to foreign MSBs or other entities. This uncertainty could be addressed through legislation that would clearly apply the BSA to entities abroad, while allowing covered foreign entities the option to comply with their jurisdiction's different requirements, so long as those requirements met minimum AML/CFT standards.