U.S. Department of the Treasury

# ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS

# ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS

## 1. Introduction

This action plan responds to Section 7(c) of Executive Order (E.O.) 14067, "Ensuring Responsible Development of Digital Assets," which calls for the development of a coordinated interagency action plan for mitigating the digital-asset-related illicit finance and national security risks as identified in the U.S. government's National Strategy for Combating Terrorist and Other Illicit Financing (Illicit Financing Strategy).[1] The Illicit Financing Strategy, which was informed by the Department of the Treasury's National Risk Assessments (NRAs),[2] outlines priorities and supporting actions to ensure that the U.S. government adapts our anti-money-laundering/countering-the-financing-of-terrorism (AML/CFT) regime to an evolving threat environment and accounts for structural and technological changes in financial services and markets.

E.O. 14067 recognizes that digital assets may pose significant illicit financing risks and commits the U.S. government to mitigating these and any other national security risks. This action plan identifies priority and supporting actions to support this commitment in line with the priorities and supporting actions identified in the Illicit Financing Strategy specific to uncovering and mitigating the misuse of digital assets by illicit actors. These priority actions include monitoring risks, working with international partners to improve cooperation on and implementation of international AML/CFT standards, strengthening our regulations and operational frameworks, and improving private sector compliance and information sharing, among others. The action plan begins with an overview of the illicit financing risks and U.S. government efforts to mitigate these risks before laying out these priority actions.

## II. Overview of Illicit Financing Risks Identified in the National Risk Assessments

The actions in this plan (see Section 4 of this report) are tailored to address the illicit financing risks that the U.S. government has identified in the NRAs related to digital assets, including virtual assets, a subset of digital assets that does not include central bank digital currencies (CBDCs) or representations of other financial assets, such as digitized representations of existing securities or deposits.[3] The NRAs, which are focused on risks that impact the U.S. financial system, did not address CBDCs given that foreign operational CBDC projects are limited in scope, and do not yet touch the U.S. financial system.

1 Within 120 days of submission to the Congress of the National Strategy for Combating Terrorist and Other Illicit Financing, the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Director of National Intelligence, and the heads of other relevant agencies shall develop a coordinated action plan based on the Strategy's conclusions for mitigating the digital-asset-related illicit finance and national security risks addressed in the updated strategy. This action plan shall be coordinated through the interagency process described in section 3 of this order. The action plan shall address the role of law enforcement and measures to increase financial services providers' compliance with AML/CFT obligations related to digital asset activities.

2 *See generally* Treasury, *Treasury Publishes National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing,* (March 1, 2022), https://home.treasury.gov/news/press-releases/jy0619, announcing (1) The 2022 National Money, Laundering Risk Assessment; (2) The 2022 National Terrorist Financing Risk Assessment; and (3) The 2022 National Proliferation Financing Risk Assessment.

3 In line with the NRAs and the Illicit Finance Strategy, this action plan uses the term virtual assets as defined by the Financial Action Task Force (FATF), the global inter-governmental body that sets international standards to prevent and address illicit financing. This term does not include CBDCs or digital representations of other financial assets. In cases where the action plan refers to both virtual assets and CBDCs, it uses the term digital assets.

Given the increase in countries studying, piloting, or launching CDBCs and the AML/CFT implications of many CBDC design features for a U.S. CBDC, if pursued, the U.S. government is assessing the illicit financing risks and national security implications of CBDCs. This effort is exploring how a CBDC could be designed to enable AML/CFT controls to mitigate illicit finance risks. Initial considerations are included in the E.O. 4(b) report on the future of money and payment systems. This action plan makes only initial references to CBDCs.

Broadly speaking, the virtual asset ecosystem has expanded rapidly since the prior NRAs were conducted in 2018. While the use of virtual assets for money laundering remains far below the scale of fiat currency and more traditional assets by volume and value of transactions, virtual assets have been used to launder illicit proceeds as described in the NRAs. The U.S. government has also seen instances of virtual assets being used to fund the activities of rogue regimes, such as the recent thefts by the Democratic People's Republic of Korea (DPRK)-affiliated Lazarus Group, and to finance terrorism, although these remain limited in scale. This section considers the key threats, vulnerabilities, and illicit financing risks related to virtual assets, which informs the following priority actions in Section 4 of this report.

## THREATS

### Money Laundering

The National Money Laundering Risk Assessment found that several threat actors, including ransomware cybercriminals, drug trafficking organizations, and fraudsters were using virtual assets, among other methods, to launder illicit proceeds.

Cybercriminals often require ransomware payments to be made in virtual assets, frequently in bitcoin. Likewise, analysis of Suspicious Activity Reports (SARs) by the Department of the Treasury's (Treasury's) Financial Crimes Enforcement Network (FinCEN) indicates that some ransomware actors have demanded payment in anonymity-enhanced cryptocurrencies (AECs),[4] requiring an additional fee for payment in bitcoin or only accepting payment in bitcoin after negotiation.[5] SAR data also shows that the cybercriminals behind the top ransomware variants commonly send funds to virtual asset service providers (VASP)[6] to be exchanged for fiat currency. The same data indicates that threat actors use foreign-located VASPs that have weak or nonexistent AML/CFT controls for ransomware-related deposits, before laundering and cashing out the funds as fiat currency. To further obfuscate the laundering of ransomware proceeds, threat actors avoid using the same wallet addresses and use

4 See page 6 for additional information on AECs.

5 FinCEN, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, (October 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

6 As defined by FATF, virtual asset service provider means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

These terms are not contained specifically in U.S. law or regulation, but for the purposes of this report they are used to describe financial institutions that provide the above financial services. VASPs in the United States qualify as money services businesses (MSBs), although some business that provide virtual asset services may be required to register with federal functional regulators, depending on the services that they are providing.

chain hopping,[7] mixing services,[8] and decentralized financial[9] (DeFi) services. Transnational criminal organizations are often the perpetrators of ransomware crimes, leveraging global infrastructure and money laundering networks to carry out their attacks.

In addition to the ransomware threat, drug trafficking organizations are growing more comfortable with darknet markets, which are used to sell narcotics and other controlled substances,[10] and the use of virtual assets to launder funds. The size and scope of drug proceeds generated on the darknet and laundered via virtual assets, however, remain low in comparison to cash-based retail street sales.

Additionally, virtual assets are increasingly being used to launder funds from fraud schemes, both in the private sector and with respect to government benefits and payments. Fraud schemes continue to be the largest driver of money laundering activity overall in terms of the scope of activity and magnitude of illicit proceeds, generating billions of dollars annually. For example, criminal actors have exchanged the illicit proceeds from online scams, unemployment insurance fraud, and business email compromise schemes, into virtual assets for laundering, among a variety of other laundering methods.

## Proliferation Financing

Virtual assets play an essential role in revenue generation and moving assets across borders although, as identified in the National Proliferation Financing Risk Assessment, there is no evidence that a proliferation network has used a virtual asset to procure a specific proliferation-sensitive good or technology as an input to a weapons of mass destruction or ballistic missile program. States and groups involved in exploiting the digital economy for sanctions evasion have used existing virtual assets, and many have developed or are trying to develop CBDCs or virtual assets backed by the state (such as Venezuela's petro) to aid in sanctions evasion. Additionally, proliferation networks are increasingly embracing certain types of virtual assets that enhance user anonymity.

DPRK's malicious cyber activities, including theft and money laundering, are an important source of revenue. For example, in March 2022, Lazarus Group, a DPRK state-sponsored cyber group, carried out the largest virtual asset heist to date, worth approximately $620 million, from a blockchain project linked to the online game Axie Infinity.[11] DPRK actors used mixers, among other methods, to launder their illicit proceeds. Additionally, DPRK actors have compromised computers and network systems to generate virtual assets (a technique known as "cryptojacking"), which could present sanctions risks to users that pay transaction fees unwittingly to these actors.

---

7 Chain hopping refers to the practice of converting one virtual asset into a different virtual asset at least once before moving the funds to another service or platform.

8 Mixing or tumbling involves the use of mechanisms to break the connection between an address sending virtual assets and the addresses receiving virtual assets. For more information, see FinCEN 2021 Ransomware Report, at 13 (Oct. 15, 2021).

9 Please see page 7 for definition of and additional information on DeFi, including details on the degree to which some DeFi services may have a controlling organization that may have AML/CFT obligations.

10 Darknet markets are Internet-based networks that individuals use special software to access in a manner designed to obscure the individuals' identity and their associated Internet activity.

11 Treasury, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768

### Terrorist Financing

According to the National Terrorist Financing Risk Assessment, U.S. authorities have identified several instances where terrorist groups and their financial supporters solicited funds in virtual assets, usually through a social media platform or other internet-based crowdsource platform. Such cases are still less prevalent than those involving traditional financial assets. This has included supporters of several international terrorist groups, as well as some domestic violent extremist groups.

For example, the Islamic State of Iraq and Syria (ISIS) has received external donations for refugee camps through various means, including virtual assets, which are converted into cash via hawaladars, where they are subsequently sent to the camps. Virtual assets can also be sent directly to ISIS supporters located in northern Syria, often to Idlib, or indirectly via Turkey, where ISIS is able to access them through virtual asset trading platforms. Additionally, some al Qaeda facilitators are exploring raising and moving funds in virtual assets. In particular, al Qaeda and affiliated groups have used social media platforms to solicit virtual asset donations as well as virtual asset vouchers to transfer money to members in Syria. As some terrorist groups operate in jurisdictions with limited financial and telecommunications infrastructure, it can be difficult to convert virtual assets to a fiat currency. Exchanging virtual assets for cash is often necessary for the funds to have utility for a terrorist group as most merchants and businesses, and many financial institutions do not accept virtual assets as a means of payment, although their use among merchants is growing.

Some foreign-based racially or ethnically motivated violent extremist groups and some domestic violent extremists have also sought to solicit or transfer funds in virtual assets or expressed interest in using virtual assets to move funds pseudonymously or in bolstering anonymity through anonymity-enhancing technologies.

## VULNERABILITIES AND ILLICIT FINANCING RISKS

Several features of virtual assets can present opportunities for misuse by illicit actors. While measures including regulation, supervision, and enforcement, among other things, can mitigate some of these vulnerabilities of virtual assets, virtual assets still pose illicit financing risks. The key illicit financing risks associated with virtual assets come from gaps in implementation of the international AML/CFT standards across countries; the use of anonymity-enhancing technologies; the lack of covered financial institutions as intermediaries—and thus the absence of AML/CFT controls— in some virtual asset transactions; and VASPs that are non-compliant with AML/CFT and other regulatory obligations.

### Cross-Border Nature and Gaps in AML/CFT Regimes across Countries

Virtual assets can be used to transfer large amounts of value across borders very quickly. Through peer-to-peer (P2P) transactions,[12] users can send virtual assets to beneficiaries regardless of geographic borders, limited only by the beneficiaries' possession of a virtual asset address and Internet-capability connection. Many users choose to store and send virtual assets through VASPs, which are able to transfer funds to counterparties globally, including other VASPs as well as unhosted

12 Please see page 6 for additional language and definition of P2P payments.

wallets, which are wallets that are not hosted by a financial institution or VASP.[13] As onboarding for VASP customers is often completed virtually, users can have their funds held in custody by or send virtual assets using foreign-based VASPs that may lack adequate regulation.

The most significant illicit financing risk associated with virtual assets stems from VASPs operating abroad with substantially deficient AML/CFT programs, particularly in jurisdictions where AML/CFT standards for virtual assets are nonexistent or not effectively implemented. Uneven and often inadequate regulation and supervision internationally allow illicit actors to engage in regulatory arbitrage, which is particularly concerning given the near-instantaneous and border-less nature of virtual asset transfers. VASPs may choose to operate in jurisdictions with minimal or nonexistent AML/CFT requirements, weak supervision of their legal frameworks, or both. Other VASPs have adopted a distributed architecture where they register in one country, have personnel in a second country, and offer services in several countries with different legal and regulatory approaches to virtual assets. This approach can complicate supervision and enforcement, which often require considerable cooperation amongst competent authorities.

## Anonymity-Enhancing Technologies

Criminals are increasingly using anonymity-enhancing technologies, such as enhanced cryptography,[14] mixers, or operation on an opaque blockchain, in the virtual asset sector. These technologies include assets, such as AECs, or services, such as mixers or tumblers, that help criminals hide the movement or origin of funds. Anonymity-enhancing technologies create challenges for investigators attempting to trace illicit funds, particularly when paired with non-compliant digital asset service providers or disintermediation, where there is no regulated financial institution to identify or report suspicious activity.[15] Providers of anonymizing services, such as mixers or tumblers, generally use software platforms that accept virtual assets and retransmit them in a manner that anonymizes the original source. While these services often operate as money transmitters and thus have regulatory reporting obligations, they may deliberately operate in a non-compliant manner to make it more difficult for regulators and law enforcement to trace illicit funds.

## Disintermediation

Many virtual assets can be self-custodied and transferred without the involvement of an intermediary financial institution, which can be referred to as disintermediated. As noted above, the use of wallets not hosted by any financial institution or VASP is commonly known as an “unhosted” or “self-hosted” wallet. Users of unhosted wallets can retain custody and transfer their virtual assets without the involvement of a regulated financial institution, and these unhosted wallet transfers of virtual assets are often referred to as P2P transactions. As described below, however, some persons despite characterizing themselves as P2P service providers or DeFi protocols may constitute a VASP and thus have AML/CFT obligations.

---

13 Please see page 6 for additional language and definition of unhosted wallets.

14 Please see page 45 of the National Money Laundering Risk Assessment for an example of the use of enhanced cryptographic technologies in virtual assets.

15 Please see next section for additional language on disintermediation.

Financial fraudsters and money launderers are increasingly seeking to evade AML/CFT controls by engaging in P2P transactions.[16] Because unhosted wallet users can transact without involving any financial services provider, many of the most important obligations of AML/CFT regimes applicable to financial institutions may not apply. This can limit authorities' collection of and access to information and reduce the effectiveness of preventive measures by financial institutions. However, P2P transfers of virtual assets may provide increased transparency of certain information when occurring on public, transparent blockchains, where transactions are often pseudonymous and associated with "addresses," or long strings of alphanumeric characters.

While the ledgers do not contain names or traditional account identifiers associated with any particular address, regulators and law enforcement can in some cases take viewable pseudonymous user and transaction information and pair it with other pieces of information to identify transaction participants. Users can also transfer funds off of the blockchain through sharing private keys, allowing another party to control the virtual assets in an unhosted wallet.

While P2P transfers occur in the ecosystem, VASPs are usually used for the exchange or withdrawal of virtual assets for fiat currency, which is commonly necessary to spend the funds. Most merchants and businesses, and many financial institutions, do not accept virtual assets as a means of payment, although their use among merchants is growing and such payments could be made from unhosted wallets.

P2P service providers, typically natural persons engaged in the business of buying and selling virtual assets rather than safekeeping virtual assets or engaging in P2P transfers on their own behalf, may have regulatory requirements depending on their precise business model. Depending on the business model, P2P exchange providers may act as money transmitters under the Bank Secrecy Act (BSA), which is the legislative framework in the United States that requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering.[17] Some of these providers have insufficient compliance programs to mitigate the risk of criminal abuse; others are intentionally operating in a manner to facilitate the exchange of illicit proceeds or evade regulation as intermediaries. For example, money mules[18] are increasingly using unhosted wallets and P2P service providers to convert between virtual assets and fiat currency and to rapidly disburse illicit funds.

Some DeFi services, meanwhile, allow for automated P2P transactions without the need for an account or custodial relationship, often through the use of smart contracts. Recent law enforcement investigations involving virtual assets have uncovered chain hopping (moving assets from one blockchain network to another via an exchange, swap, or "wrapped" asset[19]), and some of this activity has involved the use of smart contracts and other DeFi services. DeFi services often lack AML/CFT or other processes to identify customers or suspicious activity and allow layering of proceeds, or the separation of the criminal proceeds from their origin, to take place instantaneously and

16 Treasury, National Money Laundering Risk Assessment, (February 2022), p. 41, https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf.

17 FinCEN, *FinCEN Guidance*, (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

18 A money mule is someone who transfers or moves illegally acquired money on behalf of someone else, per FBI, *Money Mules*, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules.

19 "Wrapped" virtual assets are a subset of virtual assets that are created on a blockchain as a synthetic for a given token on another blockchain, thereby enabling the reference token to be used on a different blockchain.

pseudonymously. Frequently, DeFi services purport to run autonomously without the support of a central company, group, or person, despite having a controlling organization—through a decentralized autonomous organization, concentrated ownership or governance rights, or otherwise—that provides a measure of centralized administration or governance. When such an entity accepts and transmits currency, funds, or value that substitutes for currency, it may be operating as a money transmitter and have AML/CFT obligations, and may be decentralized only or partly in name.

### VASP Registration and Compliance Obligations

VASPs that operate wholly or in substantial part in the United States have AML/CFT obligations as money services businesses (MSB) because they accept and transmit value that substitutes for currency from one person to another person or location. For example, foreign-located VASPs that offer money transmission services wholly or in substantial part in the United States are required to register as MSBs and to develop, implement, and maintain an effective AML/CFT program.[20] MSBs that fail to register with FinCEN, which is responsible for administering and enforcing the BSA; implement an effective AML/CFT program; or abide by recordkeeping and reporting obligations, such as the requirement to file SARs, are more likely to be exploited by criminals without detection. Similarly, VASPs that are required, but fail, to register with federal functional regulators such as the Commodity Futures Trading Commission (CFTC) or Securities and Exchange Commission (SEC) create similar vulnerabilities.[21]

As noted above, some P2P service providers and DeFi services providers may have AML/CFT obligations if they operate wholly or in substantial part in the United States and offer money transmission services. In some cases, foreign-based VASPs have intentionally provided services to U.S. persons without proper registration, including instructing U.S.-based customers to use a virtual private network to obfuscate their location. Non-compliance on this nature represents a significant risk to the U.S. financial system and is a violation of U.S. laws and regulations.

## III. Overview of U.S. Government Efforts to Mitigate Digital Asset Illicit Financing Risks

The United States has been a leader in applying its AML/CFT framework to virtual assets domestically and advocating for appropriate AML/CFT standards for nearly a decade, both domestically and in international fora. In line with the U.S. regulatory approach of regulating financial institutions based on the financial services they provide, U.S. regulators have issued interpretive and clarifying guidance and policy statements since 2013 to help financial institutions offering virtual asset services understand their AML/CFT and sanctions compliance obligations. For example, FinCEN published guidance regarding the application of BSA rules to financial institutions offering money transmission services in virtual assets in 2013 and 2019. Other regulators, including the SEC and CFTC, have issued statements with FinCEN reminding persons engaged in activities involving virtual assets of their AML/CFT obligations under the BSA.[22] Additionally, Treasury's Office of Foreign Assets Control (OFAC)

20 31 CFR 1010.100(ff); 31 CFR 1022.380 (obligation to register with FinCEN); 31 CFR 1022.210 (obligation "to develop, implement, and maintain an effective anti-money laundering program").

21 AML/CFT obligations apply to entities defined as "financial institutions" in the BSA. These include futures commission merchants and introducing brokers obligated to register with the CFTC and broker-dealers and mutual funds obligated to register with the SEC.

22 SEC, CFTC; *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets* (October 11, 2019), https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets; https://www.cftc.gov/PressRoom/SpeechesTestimony/cftcfincensecjointstatement101119.

in 2018 clarified through an FAQ that sanctions compliance obligations are the same, regardless of whether a transaction is denominated in virtual assets or traditional fiat currency, and in 2021 published a compliance guide for the virtual asset industry.[23]

In line with this approach, U.S. regulators have been examining financial institutions providing virtual assets-related services for compliance with registration, AML/CFT, and sanctions obligations and have taken enforcement actions against non-compliant institutions. For example, in 2021 FinCEN and the CFTC announced a $100 million civil monetary penalty against BitMEX, an exchange offering virtual asset derivatives, for failing to register with the CFTC and willfully violating its U.S. AML/CFT obligations under the BSA.[24] The SEC has also taken enforcement actions against several entities and individuals for failing to register with the SEC.[25] OFAC monitors compliance with U.S. sanctions obligations. In 2021, for example, it entered into a $507,375 settlement agreement with U.S. virtual asset payment service provider BitPay for processing virtual asset transactions between the company's customers and persons located in sanctioned jurisdictions.[26]

The U.S. government also uses other tools, including law enforcement initiatives and sanctions designations, to expose and disrupt criminals misusing virtual assets and their facilitators, including VASPs. In 2021, for example, building on its existing Digital Currency Initiative, the Department of Justice (DOJ) created the National Cryptocurrency Enforcement Team (NCET) to tackle complex investigations and prosecutions of criminal misuses of virtual assets, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors. Among other cases, the NCET assisted with the February 2022 arrest of two individuals and the seizure of over $3.6 billion in virtual assets linked to the 2016 hack of a VASP.[27] OFAC levied its first sanctions designations against a digital asset service provider in 2021 for its part in facilitating ransomware payments, and has since designated 11 other targets in the digital asset ecosystem and included over 150 wallet addresses as identifiers on the List of Specially Designated Nationals and Blocked Persons.[28] In 2022, OFAC also designated its first mixer, Blender.io, in connection with the facilitation of DPRK illicit activity. and subsequently designated Tornado Cash in connection with the laundering of more

---

23 Treasury, *Sanctions Compliance Guidance for the Virtual Currency Industry*, (October 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

24 CTFC, *Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations*, (August 10, 2021), https://www.cftc.gov/PressRoom/PressReleases/8412-21.

25 See, e.g., SEC, *SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations*, (December 8, 2014), https://www.sec.gov/news/press-release/2014-273. SEC, *SEC Charges ICO Superstore and Owners With Operating As Unregistered Broker-Dealers*, (September 11, 2018), https://www.sec.gov/news/press-release/2018-185. SEC, *SEC Charges ICO Incubator and Founder for Unregistered Offering and Unregistered Broker Activity*, (September 18, 2019), https://www.sec.gov/news/press-release/2019-181. SEC, *SEC Charges Promoters of Multi-Level Digital Asset Marketing Scheme*, (August 18, 2020), https://www.sec.gov/litigation/litreleases/2020/lr24870.htm. SEC, SEC Charges Bitcoin-Funded Securities Dealer and CEO, (September 27, 2018), https://www.sec.gov/news/press-release/2018-218.

26 Treasury, "OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.

27 DOJ, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency*, (February 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

28 Specially Designated Nationals List - Data Formats & Data Schemas, (Updated August 19, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas.

than $7 billion worth of virtual assets since its creation in 2019, pursuant to Executive Order (E.O.) 13694, as amended.[29,30]

At the international level, the United States led efforts at the Financial Action Task Force (FATF), the global inter-governmental body that sets international standards to prevent and address illicit financing, to develop and adopt the first international standards on virtual assets during the United States' FATF presidency. Since 2018, the FATF has made clear that its standards apply to VASPs, and that such providers are expected to implement the same AML/CFT measures as other financial institutions, with few exceptions. In particular, the FATF has issued and updated guidance clarifying the applicability of a risk-based approach to regulating virtual assets and VASPs and published three updates on the state of implementation and the evolution of risks in the virtual asset sector. Much of this has been accomplished through the FATF's working group on virtual assets—the Virtual Assets Contact Group (VACG)—which the United States co-chairs. The U.S. government also works within other multilateral fora, such as the Group of 7 (G7) and the Financial Stability Board (FSB), and with countries on a bilateral basis, to encourage and support the implementation of the FATF standards for virtual assets and VASPs.

In addition to these efforts, the U.S. government has also been engaging through multilateral fora to establish principles for CBDCs and ensure that they align with international standards, including mitigating illicit finance risks while protecting privacy and promoting financial inclusion. Under the FATF standards, CBDCs are treated as fiat currency and, therefore, CBDCs should be designed to comply with the global AML/CFT standards currently in place. In 2021, the G7 issued a set of thirteen policy principles to guide the development of retail CBDCs, which included a principle that any CBDC needs to integrate a commitment to mitigate its use in facilitating crime.[31,32]

## IV. Priority Actions

Informed by the threats, risk, and vulnerabilities associated with digital assets noted above, as well as the four priorities identified in the Illicit Financing Strategy, this action plan lays out seven priority and supporting actions to which the U.S. government is committed. The majority of the supporting actions below continue and deepen ongoing Treasury work, such as leading at the FATF on virtual assets, taking enforcement actions against VASPs that are non-compliant with their AML/CFT obligations, using U.S. government authorities to disrupt illicit activity and the abuse of virtual assets, and supporting U.S. firms developing new financial technologies. Some of the supporting actions also include new efforts, such as preparing an illicit finance risk assessment on DeFi or convening state supervisors responsible for VASPs to promote standardization and coordination of state licensing and AML/CFT obligations. The priority supporting actions also align with the commitments made in E.O. 14067 for the United States to mitigate the illicit finance and national security risks posed by the misuse of digital assets. The Action Plan identifies lead Departments and Agencies supporting each

29 Treasury, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats,* (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768.

30 Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, (August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

31 G7, *Public Policy Principles for Retail CBDCs*, (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf

32 In 2022, the Section 4(b) report also included "compliance with AML/CFT requirements" as a principal policy objective for a U.S. CBDC system, if one were pursued.

action. Unless specified, all Departments and Agencies are considered supporting participants for the supporting actions.

***Priority Action 1: Monitoring Emerging Risks:*** The United States will continue to monitor the development of the digital assets sector and its associated risks to identify any gaps in our legal, regulatory, and supervisory regimes. These findings will inform further prioritization and resourcing of the other priority actions identified in this action plan. These efforts will include the collection and analysis of all-source information and comparison of illicit financing risks within the interagency and with foreign partners and the private sector. This work will support continued assessments of key illicit financing risks. The United States will also continue to invest in technology and training to help law enforcement, investigators, analysts, and regulators benefit from the transparency of public blockchains for AML/CFT purposes and U.S. government officials' expertise in this space.

*Supporting Actions*

- Leverage and expand the U.S. government's unique access; data sets, including BSA reporting and consumer complaint data; and expertise to identify emerging strategic risks associated with digital assets and specific threat actor uses of digital assets, and facilitate U.S. government and international partner actions to mitigate those risks and abuses. Continue to analyze BSA reporting to identify the misuse of digital assets and emerging illicit finance trends. Engage with partner nations to exchange and update views on digital assets-related illicit financing risks. (Lead: TREAS)
- Lead efforts at the FATF to monitor the virtual asset and VASP sector for material changes or developments that necessitate further revision or clarification of the FATF standards. This includes discussions on DeFi, P2P, non-fungible tokens (NFTs), and other emerging technologies. (Lead: TREAS)
- Monitor adoption of virtual assets as legal tender and CBDCs in other jurisdictions, analyze associated illicit finance risks, and engage with countries to ensure appropriate AML/CFT controls are in place. (Lead: TREAS)
- To support the Federal Reserve's CBDC research and technical experimentation efforts, consider the implications of adoption of a U.S. CBDC on AML/CFT obligations and national security (see EO 4(b) report). (Lead: TREAS)
- Continue to share relevant tactical information and analysis of emerging trends with domestic stakeholders, including law enforcement, policymakers, and financial institutions, to assist in understanding, identifying, and mitigating digital assets-related illicit finance activities.[33] (Lead: TREAS)
- Conduct ongoing analysis and outreach to inform the U.S. government's understanding of risks as Treasury prepares for the 2024 NRAs. (Lead: TREAS)
- Prepare and publish a risk assessment by February 24, 2023 on the money laundering and terrorist financing risks related to DeFi. Prepare and publish a risk assessment by July 2023 on the money laundering and terrorist financing risks related to NFTs. (Lead: TREAS)
- Accelerate training on blockchain analytics and other emerging technologies as well as relevant government databases, including consumer complaint databases, so that U.S. government investigators, analysts, and regulators, as appropriate, can continue to leverage data from public

33 FinCEN's activities in this space are consistent with its obligations pursuant to Section 6206 of the Anti-Money Laundering Act of 2020, which requires FinCEN to publish threat pattern and trend information derived from SARs at least semiannually.

blockchains to map illicit networks. Such training may also be useful for policy and other officials that do not themselves conduct analysis to understand the value and appropriate uses of this data. (Lead: TREAS, DOJ, Department of Homeland Security (DHS), Federal Functional Regulators (FFRs))

- Share expertise within the U.S. government on typologies and red flag indicators for illicit financing risks related to digital assets as well as best practices in investigating and analyzing illicit finance in digital assets. (Lead: TREAS, DOJ, DHS, FFRs)
- Continue funding foundational, use-inspired, and translational research and development in security, privacy, and accountability, and transparency issues to help detect or mitigate illicit finance. Such funded efforts will address current challenges and develop next-generation cryptographic foundations and other distributed systems security and privacy solutions. (Lead: National Science Foundation (NSF), DHS)

***Priority Action 2: Improving Global AML/CFT Regulation and Enforcement:*** Addressing significant weaknesses in AML/CFT regulation, supervision, and enforcement in foreign jurisdictions is a priority for the U.S. government in combating the illicit use of digital assets. To support this work, the U.S. government will continue to work through the FATF and other multilateral fora to promote the effective implementation of measures related to virtual assets, including regulatory efforts and robust supervision and enforcement for VASPs and others in the virtual asset ecosystem. These efforts will be complemented by bilateral engagement, to include information sharing and capacity building, as appropriate, to support countries in implementing the international AML/CFT standards for virtual assets and VASPs. The U.S. government should also help ensure that countries pursuing CBDCs have considered the AML/CFT implications and mitigated AML/CFT risks, and that these countries' AML/CFT frameworks apply to CBDCs, tailored to how the CBDC is implemented.

*Supporting Actions*

- Support the international framework developed pursuant to EO Section 8(b)(ii), which outlines how the U.S. government will engage through multilateral fora and on regional and bilateral levels to mitigate illicit finance and national security risks posed by the misuse of digital assets. It also details how the U.S. government will counter and respond to efforts by foreign adversaries to undermine international standards and promote their own objectives. (Lead: TREAS)
- Continue leading the FATF's work on virtual assets as co-lead of the VACG, which is focused on encouraging implementation of the FATF standards, such as application of the travel rule.[34] Additionally, the United States and Israel will co-lead a FATF project on the financing of ransomware trends and typologies, which aims to raise awareness on how payments for ransomware are made and how the proceeds of ransomware attacks are laundered and made available to cybercriminals. (Lead: TREAS, Supporting: DOJ, DHS, FFRs)
- Continue to work through the Egmont Group to update and improve international supervisory standards and ensure that these standards are implemented and effectively communicated to the global financial intelligence unit (FIU) community to mitigate jurisdictional arbitrage. (Lead: TREAS)

34 The travel rule refers to the requirement for VASPs to transmit certain required originator and beneficiary information when making virtual asset transfers. Please see the Interpretive Note to Recommendations 15 and 16 of the FATF Standards for more information on the travel rule (https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf).

- Lead efforts at relevant international fora, including the Egmont Group, G7, FSB, and the Bank for International Settlements, to ensure that appropriate AML/CFT controls are incorporated into best practices and policy principles while supporting user privacy in the design and regulation of CBDCs. This includes discussing key challenges and best practices in supporting countries' implementation of digital asset AML/CFT regulation with international organizations, like the International Monetary Fund, Egmont Group, World Bank, and the United Nations Office on Drugs and Crime, which have been conducting regional training sessions on this issue. (Lead: TREAS, FFRs, Department of State (STATE), as appropriate)
- Partner with G7 countries to amplify calls for implementation of the FATF standards for virtual assets and VASPs and bilaterally engage with countries to support implementation. (Lead: TREAS, Supporting: STATE)
- Engage bilaterally with countries that the U.S. government assesses will be receptive to engagement and have high illicit financing risks related to virtual assets to encourage and support implementation of the FATF standards for virtual assets and VASPs. This will include building capacity around digital asset AML/CFT regulation, supervision, and enforcement. These engagements may also include discussions on AML/CFT considerations of CBDCs if the country is pursuing one. Treasury will work with Congress to secure funding requested in the 2023 Budget to support this effort. (Lead: TREAS, Supporting: STATE)
- Share information with partners, as appropriate, to support international investigations and prosecutions on the abuse of digital assets. (Lead: TREAS, DOJ, DHS)

***Priority Action 3: Updating BSA Regulations:*** To address the illicit financing risks identified in Priority 1 of this document, Treasury will continue to evaluate its regulatory posture to ensure the U.S. AML/CFT regulatory regime can continue to safeguard the U.S. financial system from all manner of threats and illicit financial activity, whether facilitated by fiat currency or digital assets. To that end, the U.S. government, primarily through Treasury and its agency FinCEN, continuously monitors and evaluates emerging financial technologies, like digital assets, to assess whether new or revised regulations may be warranted in line with Priority 1.

*Supporting Actions*

- As required by EO Section 7(d), continue to notify relevant agencies through the interagency process of any pending, proposed, or prospective rulemakings that address digital asset illicit finance risks. (Lead: TREAS)
- Continue to review comments received in response to ongoing virtual asset-related Notices of Proposed Rulemaking[35] and address them, as appropriate, in any rules. (Lead: TREAS)
- Continue to evaluate the emergence and evolution of digital assets to determine whether any gaps exist in the current AML/CFT framework or its application. This could include continued consideration within the U.S. government of the utility and risks of lowering the $3,000 threshold

35 In particular, the Notices of Proposed Rulemaking titled "Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement to Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status" and "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets."

for the requirement to collect, retain, and transmit to other financial institutions information.[36] (Lead: TREAS)

***Priority Action 4: Strengthening U.S. AML/CFT Supervision of Virtual Asset Activities:*** It is imperative that the United States continue to lead on establishing the global model for supervision, examination, enforcement, and compliance with existing AML/CFT regulatory obligations. Treasury continues to engage with intergovernmental standard-setting bodies, such as the FATF, and with partner FIUs globally to ensure that digital asset supervision evolves in a uniform manner. Treasury is working to ensure that VASPs doing business wholly or in substantial part in the United States, wherever located, register with the requisite regulatory bodies at the state or federal level, and that they implement AML/CFT requirements.

*Supporting Actions*

- Strengthen FinCEN's existing supervisory enforcement function to increase and harmonize compliance with AML/CFT requirements, especially through examinations and related compliance and enforcement investigations and actions. (Lead: TREAS)
- Continue pursuing enforcement activity, as appropriate. Public enforcement actions, as appropriate, could encourage ongoing compliance and signal to VASPs that they will be held accountable for failing to meet AML/CFT and sanctions obligations, including registration with relevant authorities. These actions can discourage future attempts to subvert regulatory requirements and enhance pressure on some foreign jurisdictions to take parallel action under their authorities. (Lead: TREAS, DOJ, FFRs)
- Convene state supervisors responsible for VASPs to promote standardization and coordination of state licensing and AML/CFT obligations, as well as supervision for MSBs, and improve state-state and state-federal coordination more broadly. (Lead: TREAS, Supporting: CFTC, SEC, State Banking Regulators)
- As appropriate, produce guidance, alerts, and notices on concerning illicit finance trends and developments in the digital asset space to encourage the filing of SARs related to such activity and support financial institutions' compliance programs. Additionally, Treasury will continue to conduct outreach, engagement, and information sharing as appropriate with the private sector to ensure robust information exchange and identification of trends observed by Treasury to further inform compliance programs. (Lead: TREAS, Supporting: FFRs)

***Priority 5: Holding Accountable Cybercriminals and Other Illicit Actors:*** The U.S. government will continue to expose and disrupt illicit actors and address the abuse of virtual assets. Actions to disrupt such illicit activities include seizures, criminal prosecutions, civil enforcement, and targeted sanctions designations to hold cybercriminals and other malign actors responsible, as well as to expose the parts of the virtual asset ecosystem enabling illicit activity and clearly identify nodes in the ecosystem that

36 In October 2020, the Board of Governors of the Federal Reserve System and FinCEN (collectively, the "Agencies") issued a proposed rule to modify the threshold in the rules implementing the Bank Secrecy Act requiring financial institutions to collect and retain information on certain funds transfers and transmittals of funds. This rulemaking was withdrawn on September 3, 2021. (https://www.federalregister.gov/documents/2022/01/31/2021-27949/semiannual-agenda-and-regulatory-plan).

pose national security risks. Specifically, mixing services, darknet markets, and non-compliant VASPs used to launder or cash out illicit funds into fiat currency are of primary concern.

*Supporting Actions*

- Continue investigating, detecting, disrupting, and prosecuting the illicit use of virtual assets including for money laundering, ransomware, terrorist financing, fraud, theft, digital extortion activity, and sanctions evasion, and holding cybercriminals and other illicit actors accountable. (Lead: DOJ, Supporting: TREAS, DHS)
- Use Treasury tools, including sanctions and special measures, to expose and hold accountable ransomware and other actors in the ecosystem involved in or facilitating illicit activities and cut them off from the international financial system. Treasury's tools, particularly sanctions designations, can expose the role that virtual assets play in facilitating a range of malicious activity and mitigate the abuse of these emerging assets and related technologies in all domains. Treasury will also work with Congress to secure funding requested in the 2023 Budget for OFAC to support these actions. Actions to target illicit actors, such as sanctions, will continue to be made in coordination with Federal law enforcement, other U.S. government agencies, and international partners. (Lead: TREAS, Supporting: DOJ, State, DHS, Intelligence Community)
- Continue to place virtual asset wallets and addresses associated with illicit use of virtual assets on the List of Specially Designated Nationals and Blocked Persons to support industry screening for and blocking or rejecting transactions associated with blocked persons. (Lead: TREAS)

***Priority Action 6: Engaging with the Private Sector:*** The U.S. government will continue to engage with the private sector to ensure that it understands existing obligations and illicit financing risks associated with digital assets, which is critical for the private sector to effectively comply with its AML/CFT obligations, and to learn from the private sector's experience and assessment of risks. This can be accomplished through the publication of official documents, discussions, and Treasury programs that enable public-private and private-private information sharing. Collaborative work with the private sector, and between private sector entities, is a key component for detecting and countering illicit finance. During such engagements, the U.S. government can discuss and promote the private sector's use of emerging technologies to strengthen AML/CFT compliance, helping financial institutions more effectively and efficiently identify and report suspicious financial activity.

*Supporting Actions*

- Deepen engagement with the private sector to enhance its understanding of existing compliance obligations; exchange information on priority illicit finance threats, as appropriate; and continue fostering relationships with firms in the virtual asset space, to include DeFi. This can include the publication of additional guidance, advisories, or other public documents, participation in appropriate private sector events, and the organization of events such as FinCEN Exchanges, Innovation Hours, tech sprints, roundtables, and more. These events could support discussion of the U.S. AML/CFT framework for emerging technologies and the use of new technologies to support compliance with existing obligations, such as the development of travel rule compliance solutions. (Lead: TREAS)

- Expand FinCEN's 314(a) program[37] to include more VASPs, which may generate additional opportunities for engagement with the private sector and enhance law enforcement efforts. (Lead: TREAS)
- Encourage VASPs to participate in and use 314(b) voluntary information-sharing mechanisms[38] to enhance the collection and reporting of potentially suspicious transactions that involve digital assets. (Lead: TREAS)
- Enable financial institutions to improve their ability to identify threats and vulnerabilities associated with criminal activity in the virtual asset space through further information sharing on cyber vulnerabilities and illicit financing risks. Encourage them to use the range of available data and toolsets including blockchain analytics tools, to include virtual asset- specific transaction monitoring services; open-source information; commercial data; and other available tools and data that would increase the efficacy of their AML/CFT programs. Such tools could also include mechanisms to consolidate fiat currency and virtual asset transaction information. These efforts can also support Priority 7. (Lead: TREAS)

***Priority Action 7: Supporting U.S. Leadership in Financial and Payments Technology:*** The U.S. government must promote a modern and evolving domestic payments system that is transparent and efficient, supports innovation, and maintains U.S. technological leadership, while safeguarding the integrity of our financial system and our national security. Real-time payment solutions and digital channels, such as same-day automated-clearing house transactions and permissioned blockchain-based payment systems, are examples of the rapid pace of innovation that appears to be reshaping domestic and global transfers.

*Supporting Actions*

- Consider additional ways to modernize the U.S. payments infrastructure, as per the section EO 4(b) report. (Lead: All)
- Work with interagency partners and Congress to implement recommendations stemming from the President's Working Group on Financial Markets on Stablecoins.[39] (Lead: TREAS)
- Continue to collaborate with FFRs to support U.S. firms developing new financial technologies through regulatory and supervisory guidance, symposia, tech sprints, FinCEN Innovation Hours, and other means. (Lead: TREAS and FFRs, Supporting: DHS)
- Fund research and development into technological foundations for future digital financial and payments systems, while supporting various system solutions to address networking, security, privacy, and resiliency challenges of existing financial and payment systems. (Lead: NSF, DHS)

---

37 31 CFR Part 1010.520; Section 314(a) of the USA PATRIOT Act enables Treasury to reach out to financial institutions to locate accounts and transactions of persons identified by law enforcement that may be involved in terrorism or money laundering. See FinCEN, FinCEN'S 314(a) Fact Sheet (Feb. 22, 2022), https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf. While several VASPs that fall under the definition of trust companies currently participate in the 314(a) program, FinCEN is considering expanding the Section 314(a) program to include additional VASPs.

38 USA PATRIOT Act Section 314(b) permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.

39 Treasury, *President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins* (Nov.1, 2021), https://home.treasury.gov/news/press-releases/jy0454.

## V. Future Engagement

The digital asset ecosystem is rapidly evolving, and the U.S. government is committed to continuing to monitor emerging risks through governmental efforts and engagement with international and private sector partners, which will inform other potential actions to mitigate these risks. Input from these stakeholders aids the U.S. government in effectively mitigating the illicit financing and national security risks related to digital assets. In particular, Treasury anticipates future engagement to discuss, among other things:

*Illicit Finance Risks*

- Has Treasury accurately articulated the illicit financing risks associated with digital assets? Please list any key illicit financing risks that we have not raised in this Action Plan or the National Risk Assessment.
- How might future technological innovations in digital assets present new illicit finance risks or mitigate illicit finance risks?
- What are the illicit finance risks related to non-fungible tokens?
- What are the illicit finance risks related to DeFi and P2P payment technologies?

*AML/CFT Regulation and Supervision*

- What additional steps should the United States government take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals?
- Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity?
- What existing regulatory obligations in your view are not or no longer fit for purpose as it relates to digital assets? If you believe some are not fit for purpose, what alternative obligations should be imposed to effectively address illicit finance risks related to digital assets and vulnerabilities?
- What regulatory changes would help better mitigate illicit financing risks associated with digital assets?
- How can the U.S. government improve state-state and state-federal coordination for AML/CFT regulation and supervision for digital assets?
- What additional steps should the U.S. government consider to combat ransomware?
- What additional steps should the U.S. government consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies?
- What steps should the U.S. government take to effectively mitigate the illicit finance risks related to DeFi?

*Global Implementation of AML/CFT Standards*

- How can Treasury most effectively support consistent implementation of global AML/CFT standards across jurisdictions for digital assets, including virtual assets and virtual asset service providers?
- Are there specific countries or jurisdictions where the U.S. government should focus its efforts,

through bilateral outreach and technical assistance, to strengthen foreign AML/CFT regimes related to virtual asset service providers?

*Private Sector Engagement and AML/CFT Solutions*

- How can Treasury maximize public-private and private-private information sharing on illicit finance and digital assets?
- How can the U.S. Department of the Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?
- How can Treasury encourage the use of collaborative analytics to address illicit financing risks associated with digital assets while also respecting due process and privacy?
- What technological solutions designed to improve AML/CFT and sanctions compliance are being used by the private sector for digital assets? Can these technologies be employed to better identify and disrupt illicit finance associated with digital assets and if so, how?
- Are there additional steps the U.S. Government can take to promote the development and implementation of innovative technologies designed to improve AML/CFT compliance with respect to digital assets?
- How can law enforcement and supervisory efforts related to countering illicit finance in digital assets better integrate private sector resources?
- How can Treasury maximize the development and use of emerging technologies like blockchain analytics, travel rule solutions, or blockchain native AML/CFT solutions, to strengthen AML/CFT compliance related to digital assets?
- How can financial institutions offering digital assets better integrate controls focused on fiat currency and digital asset transaction monitoring and customer identification information to more effectively identify, mitigate, and report illicit finance risks?

*CBDC*

- How can Treasury most effectively support the incorporation of AML/CFT controls into a potential U.S. CBDC design?