# REPORT TO CONGRESS FROM THE SECRETARY OF THE TREASURY ON INNOVATIVE TECHNOLOGIES TO COUNTER ILLICIT FINANCE INVOLVING DIGITAL ASSETS

THE DEPARTMENT OF THE TREASURY

1789

# REPORT TO CONGRESS FROM THE SECRETARY OF THE TREASURY ON INNOVATIVE TECHNOLOGIES TO COUNTER ILLICIT FINANCE INVOLVING DIGITAL ASSETS

*As Part of the Implementation of the Guiding and Establishing National Innovation for U.S. Stablecoins Act, 2025*

**United States Department of the Treasury**

**March 2026**

# Table of Contents

## Section 1: Introduction

Digital assets play a crucial role in global innovation and economic development. The Trump Administration is restoring U.S. leadership in digital asset technologies and promoting their responsible use and growth. The Administration is committed to countering illicit finance—such as money laundering or sanctions evasion—involving this industry, which threatens U.S. national security, harms U.S. digital asset users, and tarnishes the reputations of legitimate industry actors. This report outlines the Department of the Treasury's (Treasury) findings regarding the use and potential use of innovative and novel methods, techniques, and strategies by financial institutions to counter illicit finance related to digital assets. It also makes recommendations, including legislative, regulatory, and other proposals.

On July 18, 2025, President Trump signed the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act into law. In addition to setting out a comprehensive regulatory framework for payment stablecoin issuers in the United States, the GENIUS Act tasked Treasury with researching innovative or novel models, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity, including money laundering, involving digital assets.[1] Treasury recognizes that financial institutions harnessing responsible innovation will increase the security of the U.S. financial system, deter bad actors, and improve the ability of law enforcement and national security agencies to combat illicit finance related to digital assets. By supporting responsible use of novel tools and techniques, Treasury aims to improve the effectiveness of the anti-money laundering and countering the financing of terrorism (AML/CFT) regulatory regime.

In line with the GENIUS Act's requirements, on August 18, 2025, Treasury issued a public request for comment (RFC) to identify innovative tools, techniques, and strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity involving digital assets. The GENIUS Act specifically identified artificial intelligence (AI), digital identity, blockchain analytics, and application program interfaces (APIs) as specific tools and technologies for consideration.[2] Treasury solicited public feedback from August to October 2025. Treasury reviewed and considered more than 220 comments from industry associations, credentialing services, blockchain intelligence companies, and other entities and individuals that responded to Treasury's RFC. Treasury conducted additional research on these and other innovative tools.

As part of drafting this report, Treasury considered stakeholder feedback, including from financial institutions and law enforcement, through industry outreach and public-private partnership conversations. As required by the GENIUS Act, Treasury considered, and this report articulates, the primary risks posed by illicit actors' abuse of digital assets, as well as sources of illicit activity. Also, as required by the GENIUS Act, this report discusses the extent to which distributed ledgers, mixers, tumblers, and similar services mix payment stablecoins to obfuscate illicit activity. Finally, it discusses decentralized finance (DeFi).

[1] Section 9(e) of the GENIUS Act requires that Treasury submit a report on these topics to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives. This report fulfills the requirement.

[2] 90 FR 40148, https://www.federalregister.gov/documents/2025/08/18/2025-15697/request-for-comment-on-innovative-methods-to-detect-illicit-activity-involving-digital-assets.

# Section 2: Risk Assessment

## Overview

The digital asset ecosystem has grown substantially in recent years.[3] The number of successful monthly transactions on public blockchains reached 3.8 billion in early 2025, a 96 percent year-over-year increase.[4] As part of this growth, an increasing number of companies have begun to offer financial services related to digital assets while financial institutions continue to evaluate digital asset-related products and services, including offering to custody digital assets, creating exchange-traded products that track the price of specific digital assets, and issuing their own digital assets like stablecoins. Generally, these financial institutions and firms have anti-money laundering/countering the financing of terrorism (AML/CFT) obligations under the Bank Secrecy Act (BSA) and firms that are U.S. persons are required to comply with sanctions administered by the Office of Foreign Assets Control (OFAC).[5]

*Spotlight: National Illicit Finance Risk Assessments*

Treasury published its latest National Risk Assessments on Money Laundering, Terrorist Financing, and Proliferation Financing in March 2026. These assessments highlighted digital asset-related risks, including money launderers misusing digital asset kiosks, North Korean hacking of digital asset service providers (DASPs), foreign terrorist groups soliciting funds in digital assets, and other threats.

[3] This report uses the terms digital assets and digital asset service provider (DASP) throughout. As defined in the GENIUS Act, the term digital asset means any digital representation of value that is recorded on a cryptographically secured distributed ledger. The term DASP (A) means a person that, for compensation or profit, engages in the business in the United States (including on behalf of customers or users in the United States) of—(i) exchanging digital assets for monetary value; (ii) exchanging digital assets for other digital assets; (iii) transferring digital assets to a third party; (iv) acting as a digital asset custodian; or (v) participating in financial services relating to digital asset issuance; and (B) does not include—(i) a distributed ledger protocol; (ii) developing, operating, or engaging in the business of developing distributed ledger protocols or self-custodial software interfaces; (iii) an immutable and self-custodial software interface; (iv) developing, operating, or engaging in the business of validating transactions or operating a distributed ledger; or (v) participating in a liquidity pool or other similar mechanism for the provisioning of liquidity for peer-to-peer transactions.

[4] a16zcrypto, "State of Crypto Index," https://a16zcrypto.com/stateofcryptoindex. These data serve as a proxy for activity across certain blockchains (specifically, Ethereum, Polygon, Solana, Avalanche, Fantom, Celo, Optimism, Base, and Arbitrum).

[5] OFAC sanctions regulations apply to all U.S. persons, including digital asset exchanges, technology companies, software developers, or other digital asset industry participants, that are subject to U.S. jurisdiction. The key terms of each sanctions program are defined in the implementing regulations or Executive Orders, as appropriate. The term "U.S. persons" is defined in many implementing regulations to include "any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States." Additionally, non-U.S. persons are also subject to certain OFAC prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions.

Individuals and businesses use digital assets for a variety of legitimate purposes, including investments, remittances, and payment for goods and services. However, like any medium of exchange, illicit actors can abuse digital assets to raise and transfer funds. The ability to transfer assets quickly across borders and the perception of anonymity make digital assets attractive to illicit actors.

## Threats

Threat actors, including fraudsters and transnational criminal organizations, the Democratic People's Republic of Korea (DPRK), ransomware actors, sanctions evaders, and others, abuse digital assets to launder illicit proceeds and cause harm to U.S. national security.

Digital asset investment schemes are a particularly damaging form of investment fraud. In these scams, perpetrators often initiate communication by messaging victims on social media, dating platforms, or by text message, sometimes claiming to have the wrong number.[6] Transnational Criminal Organizations perpetrate these scams by operating industrial-scale scam centers, often located outside of the United States in countries such as Burma, Cambodia, and Laos, that target Americans. In 2024, victims reported over $9 billion in losses from digital assets-related fraud to the FBI's Internet Crime Complaint Center (IC3).[7] IC3 estimated that, of this $9 billion total, losses from digital asset investment schemes accounted for $5.8 billion, a 47 percent increase over the prior year.[8]

DPRK cybercriminals have generated billions of dollars of revenue in digital assets through theft, and the DPRK relies on schemes involving the use of digital assets to fund the regime's weapons of mass destruction and ballistic missiles program.[9] The DPRK uses complex social engineering schemes to compromise entities' networks, posing a persistent threat to DASPs around the globe. For example, in February 2025, DPRK cybercriminals stole digital assets valued at $1.5 billion from a DASP, the largest digital asset heist to date.[10] From January 2024 to September 2025, the DPRK stole at least $2.8 billion in digital assets.[11]

Ransomware is a type of malicious software that encrypts a victim's data or systems and demands payment before access is restored. Ransomware criminals continue to mainly demand payments in digital assets and direct victims to send ransom payments to specific digital asset wallet addresses. The value of ransomware payments—the vast majority of which involve digital assets—reported to Treasury's Financial Crimes Enforcement Network (FinCEN) reached an all-time high of $1.1 billion in 2023 before declining to roughly $734 million in 2024, due to a

[6] *See* FinCEN, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering" (Sept. 8, 2023) FinCEN Alert, FIN-2023-Alert005, September 8, 2023.

[7] IC3 is the primary destination for the American public to report cyber-enabled crime and fraud.

[8] FBI, "Internet Crime Report 2024," https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[9] *See* Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (Mar. 2025), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[10] *See* Internet Crime Complaint Center (IC3) | North Korea Responsible for $1.5 Billion Bybit Hack.

[11] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," pg. 25, https://msmt.info/Publications/detail/MSMT%20Report/4221.

variety of factors including law enforcement actions and disruptions of major ransomware groups, and stronger victim defenses and responses.[12]

U.S. adversary jurisdictions under significant economic restrictions due to U.S. and international sanctions, such as Russia and Iran, also abuse digital assets, though these adversaries continue to rely primarily on fiat currency, leveraging digital assets when possible. For example, a Russian entity created a ruble-backed stablecoin to facilitate cross-border settlements for the purpose of evading sanctions, resulting in the United States and United Kingdom identifying and sanctioning the stablecoin issuer.[13] In other cases, Iranian actors have facilitated the purchase of millions of dollars in digital assets for illicit oil sales for the Iranian regime.[14]

While digital assets are not the primary method used by other threat actors such as drug traffickers and terrorist groups, they have become more popular in recent years in line with the increased adoption of digital assets; such actors use digital assets for transfers or purchases, as well as to launder assets obtained from illegal activity.[15]

## Vulnerabilities

As described above, illicit actors use digital assets to facilitate and profit from crime. In many instances, these actors leverage a combination of the vulnerabilities explained below—such as DASPs located in foreign jurisdictions that lack robust AML/CFT obligations and DASPs that do not comply with U.S. regulatory obligations—to launder illicit proceeds.

### *Jurisdictional Arbitrage*

Uneven and often inadequate regulation and supervision across jurisdictions allow certain DASPs and illicit actors to engage in regulatory arbitrage, where companies or individuals exploit differences between laws and regulations in different jurisdictions and systems to avoid stricter rules without changing their underlying economic activity. The U.S. financial system may be exposed to risks related to DASPs operating from jurisdictions with weak or nonexistent AML/CFT obligations. Six years ago, the Financial Action Task Force (FATF), an international standards-setting body for AML/CFT and counter-proliferation financing, clarified the application of its global standards on AML/CFT to digital assets and DASPs.[16] However, certain jurisdictions continue to have weak or non-existent AML/CFT standards for digital asset services providers.[17] Illicit actors take advantage of these gaps and may seek out DASPs that do not require, among other things, the collection and verification of customer identification documents as part of an onboarding process or to transfer funds.

[12] FinCEN, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024," December 2025, https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf.
[13] Treasury, "Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals," https://home.treasury.gov/news/press-releases/sb0225.
[14] Treasury, "Treasury Targets Financial Network Supporting Iran's Military," https://home.treasury.gov/news/press-releases/sb0248.
[15] To find additional, detailed information on threat actors' abuse of digital assets, please reference Treasury's National Risk Assessments on Money Laundering, Terrorist Financing, and Proliferation Financing.
[16] *See,* Financial Action Task Force, "Virtual Assets," https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/Virtual-assets-fatf-standards.html.
[17] The FATF uses the term virtual assets, but this report, in line with the GENIUS Act, uses the term digital assets.

Some DASPs may obfuscate their location, including by maintaining an unclear corporate structure or one that spans several different countries. Such DASPs can have a distributed architecture where they register in one country, have personnel in a second country, maintain data on servers located in a third country, and offer services in several countries with different legal and regulatory approaches to digital assets. Such entities may not be subject to appropriate supervision, which complicates oversight of complex entities holding separate licenses for operations in numerous jurisdictions. Certain services may claim to be regulated while they are only licensed as legal entities in a jurisdiction.

### *Failure to Comply with U.S. Obligations*

When DASPs fail to comply with their AML/CFT and sanctions obligations, illicit actors can more easily exploit them for nefarious purposes. For example, DASPs may claim not to be subject to U.S. jurisdiction and fail to register as a money services business with FinCEN as required under 31 CFR 1022.380, despite doing business wholly or in substantial part in the United States. Certain DASPs may also fail to implement appropriate AML/CFT controls or comply with sanctions obligations, allowing illicit actors to use these entities to move digital assets. Other DASPs may direct their customers to conceal their U.S. presence when establishing accounts at onboarding or may claim not to be regulated financial institutions subject to the BSA.

Also, while digital asset kiosks[18] can be a simple and convenient way for customers to access digital assets, they are increasingly abused.[19] This rise in illicit activity may be related, in part, to substantial rates of non-compliance with AML/CFT regulations by kiosk operators,[20] which can render digital asset kiosks especially vulnerable to abuse by scammers and other financial criminals. According to law enforcement, scammers have directed victims to specific digital asset kiosks, likely to avoid other digital asset kiosk operators with strong AML/CFT controls. In 2024, there were more than 10,900 complaints to IC3 on the use of digital asset kiosks, with reported victim losses of approximately $246.7 million.[21]

### *Mixers and Other Obfuscation Services*

As part of the GENIUS Act, Congress directed Treasury to report on "the extent to which transactions on distributed ledgers, digital asset mixing services, tumblers, or other similar services that mix payment stablecoins in such a way as to make such transaction or the identity of the transaction parties less identifiable may facilitate illicit activity."[22]

Mixers obfuscate transactional information that could otherwise be viewable on a public blockchain.[23] Mixing services may involve centralized or decentralized mechanisms and may be

[18] Digital asset kiosks are self-service electronic terminals that let customers buy and sell digital assets for cash. They are often called crypto ATMs.

[19] FinCEN, FinCEN Notice, FIN-2025-NTC1, August 4, 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf.

[20] FinCEN, FinCEN Notice, FIN-2025-NTC1, August 4, 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf.

[21] FBI, IC3, "Internet Crime Report 2024," https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf, p. 36.

[22] Section 9(e)(D) of the GENIUS Act.

[23] "Strengthening American Leadership in Digital Financial Technology," https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, pg. 103.

effectuated using several techniques: pooling or aggregating digital assets from multiple individuals, wallets, or accounts into a single transaction or set of transactions; splitting an amount into multiple amounts and transmitting the digital assets as a series of smaller independent transactions; or leveraging code to coordinate, manage, or manipulate the structure of the transaction, among other methods.[24] Certain mixing services may be clearly advertised as a way to evade AML/CFT and sanctions requirements.

Lawful users of digital assets may leverage mixers to enable financial privacy when transacting through public blockchains.[25] For instance, individuals may use mixers to protect sensitive information on personal wealth, business payments, or charitable donations from appearing on a public blockchain. As consumers increase their use of digital assets for payments, individuals may want to use mixers to maintain more privacy of their consumer spending habits. In addition, digital asset services that take custody of user funds and accept and transmit value are currently required to register with FinCEN as money services businesses (MSBs), maintain records, and file suspicious activity reports. This includes custodial mixers, which—when compliant with recordkeeping requirements—could provide unique information such as customer identities, off-chain data on transactions, and behavioral patterns related to illicit digital asset flows upon request to regulators or law enforcement.

Criminals commonly use tools like mixing (as well as bridging, where certain assets are exchanged for others on a different blockchain through entities known as bridges, and swapping, where one asset is directly exchanged for another) to introduce challenges for investigators attempting to trace illicit digital assets, frustrating law enforcement investigations as well as DASPs' transaction monitoring and tracing efforts. Mixing is frequently used by DPRK cyber actors, money launderers, ransomware actors, participants in darknet markets, and other illicit actors.[26] For example, in one case, a hacker leveraged multiple techniques to launder stolen funds, including depositing the stolen funds into a variety of darknet markets as well as depositing a portion of the criminal proceeds into digital asset mixing services.[27] DPRK cyber actors are particularly adept at using mixers to launder funds. For instance, they swap stolen tokens using decentralized exchanges and then mix them before consolidating the digital assets in self-hosted wallets with limited interdiction opportunities. These DPRK actors then mix the stored assets again as part of a combination of obfuscation techniques, including further bridging and swapping, before cashing out. DPRK actors rapidly move funds through mixers and other obfuscation techniques.[28]

[24] Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf, pg. 10.

[25] "Strengthening American Leadership in Digital Financial Technology," https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, pg. 107.

[26] Treasury, "2024 National Money Laundering Risk Assessment," https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf, pg. 63.

[27] DOJ, "Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency," https://www.justice.gov/archives/opa/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen.

[28] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," pg. 42-43, https://msmt.info/Publications/detail/MSMT%20Report/4221.

Stablecoins are often used as one element of a complex laundering process that includes the use of mixers, such as the one described above. Illicit actors use stablecoins in the laundering process, particularly when moving digital assets between blockchains and/or in the last phase of their transaction as they convert illicit digital assets into fiat currency, potentially through over-the-counter brokers who prefer stablecoins.[29]

To make the stablecoins they acquire appear as "clean" as possible, illicit actors commonly channel other digital assets, such as Bitcoin, that have been obtained through theft or fraud through a mixer[30] and then quickly swap those assets into stablecoins. These stablecoins are then transferred to a new digital asset wallet, breaking a direct, easily traceable connection to the original Bitcoin linked to criminal activity. This tactic can be used to circumvent AML/CFT and sanctions controls and to provide deniability to the party ultimately converting the illicit stablecoins to fiat currency. According to Treasury analysis, since May 2020, more than $37.4 billion withdrawals from over 50 bridges have been denominated in the two largest stablecoins by market capitalization. During the same period, the same bridges received approximately $1.6 billion in deposits originating from mixing services. Over half of those deposits (more than $900 million) were into a specific bridge, which faced scrutiny for failing to intervene in swaps made on the platform by the DPRK as DPRK-linked actors laundered the proceeds of a digital asset heist. The depositing of stablecoins directly into mixers for illicit purposes appears to be low, although illicit actors may apply other obfuscation techniques to stablecoins.

In 2023, FinCEN issued a notice of proposed rulemaking (NPRM) that contemplated requiring financial institutions to implement certain recordkeeping and reporting requirements related to transactions involving mixing services.[31] The President's Working Group (PWG) Report on Digital Assets, published July 2025, recommended that Treasury consider next steps on this proposal in line with Administration priorities to counter illicit finance risks while protecting privacy and reducing regulatory burden.[32]

## Section 3: U.S. Regulatory Framework & Innovation Priorities

The BSA[33] is designed to combat money laundering, the financing of terrorism, and other illicit finance activity risks. To fulfill the purposes of the BSA, Congress has authorized the Secretary

[29] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," pg. 44, https://msmt.info/Publications/detail/MSMT%20Report/4221.

[30] OFAC, "Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency," https://home.treasury.gov/news/press-releases/jy1933.

[31] "Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern," 88 FR 72701 (October 23, 2023).

[32] "Strengthening American Leadership in Digital Financial Technology," https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, pg. 107.

[33] Parts of the Currency and Foreign Reporting Act of 1970 (Pub. L. No. 91-508, 121, 84 Stat. 1114 (1970)), its amendments, and other related statutes have come to be referred to as the "Bank Secrecy Act." For its purposes, the GENIUS Act defines the "Bank Secrecy Act" to mean (A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b); (B) chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.); and (C) subchapter II of chapter 53 of title 31, United States Code. 12 U.S.C. § 5901(2).

of the Treasury (Secretary) to, among other things, administer the BSA and require financial institutions to keep records and file reports that, among other purposes, “are highly useful in criminal, tax, or regulatory investigations, risk assessments, or proceedings,” or in the conduct of “intelligence or counterintelligence activities, including analysis, to protect against terrorism.”[34] The BSA also authorizes the Secretary to require each financial institution to establish an AML program to ensure compliance with the BSA and guard against money laundering and terrorist financing. The Secretary has the authority to “establish appropriate frameworks for information sharing among financial institutions, their agents and service providers, their regulatory authorities, associations of financial institutions, the Department of the Treasury, and law enforcement authorities to identify, stop, and apprehend money launderers and those who finance terrorists.”[35] The Secretary has delegated the authority to implement, administer, and enforce compliance with the BSA and its associated regulations to the Director of FinCEN.[36]

In 2021, Congress enacted the Anti-Money Laundering Act of 2020 (AML Act) as a part of the William M. (Mac) Thornberry National Defense Authorization Act.[37] A key objective of the AML Act was to strengthen and modernize the AML/CFT regulatory framework, including through encouraging “technological innovation and the adoption of new technology by financial institutions.”[38] The AML Act also amended the BSA to further solidify the inclusion of digital assets into the U.S. AML/CFT framework by expanding key definitions to account for “value that substitutes for currency.”[39] An entity generally has BSA obligations if it qualifies as a financial institution under the BSA, which is based on the entity’s activities, regardless of whether the activity is in fiat, digital assets, or both. Participants in the digital asset ecosystem may meet the definition of one or more financial institution types under the BSA (e.g., MSBs, insured banks, trust companies, futures commissions merchants, broker-dealers) but are often treated by FinCEN as MSBs.[40]

[34] 31 U.S.C. § 5311(1); *see also* 31 U.S.C. § 5318(g).

[35] 31 U.S.C. §§ 5311(5) (2024); *see also* 31 U.S.C. § 310(d).

[36] *See* Treasury Order 180-01, paragraph 3(a) (January 14, 2020), https://home.treasury.gov/about/general-information/orders-and-directives/treasury-order-180-01; *see also* 31 U.S.C. 310(b)(2)(I) (providing that FinCEN Director “[a]dminister the requirements of subchapter II of chapter 53 of this title, chapter 2 of title I of Public Law 91-508, and section 21 of the Federal Deposit Insurance Act, to the extent delegated such authority by the Secretary”).

[37] The AML Act was enacted as Division F, §§ 6001-6511, of Pub. L. No. 116-283 (2021).

[38] *See* AML Act, § 6002(3) (Purposes).

[39] *See* AML Act § 6102(d). Note that regulatory definitions pre-dating the AML Act recognized that BSA obligations could apply to activity involving “value that substitutes for currency.” See Financial Crimes Enforcement Network; Amendments to the Bank Secrecy Act Regulations-Definitions and Other Regulations Relating to Money Services Businesses, 74 Fed. Reg. 22129, 22137 (May 12, 2009) (discussing current definition of “money transmitter” and proposed inclusion of “value that substitutes for currency,” among other changes); Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43585 (July 21, 2011) (adopting definition); FinCEN, FIN-2019-G001, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies 4 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf; FinCEN, FIN-2013-G001.

[40] *See, e.g.*, 31 CFR 1010.100(h) (defining broker or dealer in securities), 1010.100(bb) (defining introducing broker-commodities), 1010.100(ff) (defining money services business). *See* FinCEN, FIN-2019-G001, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies 4 (May 9, 2019), for an explanation of why digital asset service providers may be considered MSBs: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

## Policy Priorities

A technology-neutral, risk-based approach to AML/CFT regulation is fundamental to Treasury's policy approach. Regulations implementing the BSA generally do not require institutions to employ particular methods or technologies to comply with AML/CFT obligations. Well-governed technology is a force multiplier for combating illicit finance, and investments by industry in innovative tools such as artificial intelligence (AI), digital identity, blockchain analytics, and APIs can produce positive, long-term results for the fight against financial crime. New technologies can reduce friction for legitimate customers and more effectively target illicit actors. The Administration is committed to empowering financial institutions to focus their resources on effectively addressing their unique risks and using technologies to do so. Financial institutions, including DASPs, should be clearly supervised in accordance with the risk-based approach, dedicating their most substantial resources to high-risk areas and deprioritizing lower risks.

Treasury will take specific steps in 2026 and beyond to support financial institutions' use of innovative tools, techniques, and strategies to combat illicit finance related to digital assets, which will assist both the private sector and government authorities in better identifying and disrupting financial crime. Having considered the responses to the RFC, Treasury's research and risk assessments, stakeholder input, and experience from Treasury's prior work on innovation and related issues, Treasury will implement the recommendations outlined in this report. In many cases, the specific recommendations related to these technologies are captured by three overarching principles.

***Overarching Policy Principles***

1. **Promote responsible innovation in AML/CFT.** Treasury will promote the use of the latest technologies by financial institutions for compliance.

2. **Collaborate with key stakeholders on emerging technologies.** Treasury will collaborate with financial supervisors to ensure financial institution examiners catalyze innovation to support AML/CFT programs.

3. **Coordinate and harmonize requirements.** Treasury will collaborate with NIST and international bodies to clarify technical principles and recommended standards to facilitate the adoption of emerging technologies.

Treasury is committed to taking practical action to support these principles. Initially, Treasury will use a range of tools to promote the use of technologies by financial institutions for compliance, including convening institutions to share ideas and best practices, working with other government agencies, and issuing policy documents, including guidance.

Secondly, Treasury will work with financial supervisors for AML/CFT to foster innovation and ensure the agencies that regulate, examine, and supervise financial institutions for AML/CFT can and do apply the greatest resources to their greatest risks and use technology to do so.[41] Treasury and these agencies will ensure that innovative tools are properly and fairly assessed.

Finally, Treasury will collaborate with other federal agencies and standard-setting bodies to facilitate the research, development, and adoption of novel and innovative tools for AML/CFT and sanctions purposes, such as digital identity and artificial intelligence, by providing clear technical principles and standards to the private sector and government.

## Section 4: Artificial Intelligence

### Overview

AI is defined in the National Artificial Intelligence Initiative Act of 2020 as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[42] AI comprises both traditional machine learning methods, in which statistical models are often trained on a dataset with input and output parameters, and newer forms of AI, such as Generative AI (GenAI). GenAI differs from traditional forms of AI in its ability to create new inferences and content based on what is learned from training data.

### Uses by Financial Institutions

Financial institutions currently use AI for a variety of purposes, including monitoring fraudulent transactions and suspicious activity, and for certain other AML/CFT compliance functions. Increasingly, financial institutions are using or testing cutting-edge technologies such as GenAI to perform certain compliance tasks. While more traditional machine learning tools are used by financial institutions to learn and perform predictive analysis and inferences from structured datasets based on transaction and other data, GenAI tools using Large Language Models (LLMs) are better adapted to tasks that involve natural language prompts and interactions with unstructured data. For instance, financial institutions are experimenting with GenAI applications that can be used to assist AML/CFT compliance personnel at financial institutions with completing case reviews, investigating suspicious activity, and even drafting suspicious activity report (SAR) narratives. Compliance personnel have used GenAI tools to perform faster and deeper synthesis and analysis of large amounts of data and have leveraged LLMs to automate adverse media and sanctions screening checks, shortening the time required to complete complex investigations and streamlining routine tasks. In response to the RFC, private sector respondents largely expressed confidence that AI—inclusive of machine learning and advanced AI—tools are

[41] The supervisory agencies also engage in a range of activities to foster innovation and support the appropriate use of digital assets and innovative technology. For example, on October 21, 2025, the Board of Governors of the Federal Reserve hosted a Payments Innovation Conference, which brought together leading industry experts to share perspectives on the evolving landscape of money and payments. As another example, the National Credit Union Association (NCUA) issued guidance on Relationships with Third Parties that Provide Digital Asset Services in 2021 and Federally Insured Credit Union Use of Distributed Ledger Technologies in 2022, which encouraged the use of these technologies when implemented in a safe and sound manner. Most recently, NCUA released a new Artificial Intelligence Resources website to support credit union understanding and opportunities in this evolving space.

[42] *See* National Artificial Intelligence Initiative Act of 2020, Pub. L. No. 116-283, 134 Stat. 4523 (2021); Removing Barriers to American Leadership in Artificial Intelligence – The White House.

or soon will be transformative for financial institutions' AML/CFT compliance. Financial institutions are considering how to adopt these innovative technologies for compliance purposes and to better understand the new risks they may introduce to their operations.

Financial institutions also may use AI tools as part of their customer onboarding and identification process, to scrutinize synthetic attempts to bypass customer due diligence controls (such as analyzing login behavior, device signals, and other identifiers), review customer-submitted identity documents, and leverage live video verification to detect so-called "deepfake" media. AI tools are being used by financial institutions to create customer risk scores based on and responsive to customer transaction activity. Financial institutions are also, in some cases, using AI tools to review transactions and other activities with the aim of reducing the number of false positives in transaction alerts.

DASPs also highlighted unique use cases for AI tools for AML/CFT compliance. Industry highlighted that AI-powered models can be efficient at analyzing blockchain transaction patterns, simulating money laundering scenarios, and learning from and adapting to evolving criminal money laundering tactics, techniques, and procedures. AI tools can also be used to perform entity resolution through graph analysis to map connections among wallets, exchanges, and off-blockchain actors. [43] Such analysis can uncover complex activity among multi-jurisdictional networks that may evade detection by legacy, "rules-based" systems that rely on more rigid heuristics for the detection of illicit activity.

Financial institutions, DASPs, and vendors also highlighted that AI tools could help streamline the detection of illicit patterns, since AI models could learn types and sequences of transactions that indicate "chain-hopping" behavior for money laundering or detect patterns consistent with "smurfing" activity, whereby structuring takes place through small deposits across multiple wallet accounts. AI tools' strengths for countering illicit finance stem from their ability to learn from the use of large and diverse data sets, and their ability to classify novel illicit financial activity in real time from this data, which can allow for faster and more effective assessment of risks and interdiction of illicit activity. There are, for example, certain tools that can proactively interdict fraudulent transactions in real time by using machine learning algorithms to identify patterns that indicate a customer's digital asset wallet is interacting with a scam website.

*Challenges*

Private sector feedback outlined concerns about the practical and regulatory challenges of using data to train and improve AI models, the costs of implementing new systems, and regulatory uncertainty in the face of these novel technologies. Respondents also noted the adversarial risks of AI tools to further financial fraud and scams, and how AI tools could be used to counter these risks if supported by the government.

Data quality, governance, and validation concerns remain barriers to the implementation of AI tools. AI models can operate as a "black box", obscuring decision-making processes by the models that can, among other things, complicate compliance teams' ability to justify or explain

[43] Entity resolution is the process of determining whether multiple records are referencing the same real-world thing, such as a person, organization, address, phone number, or device.

decisions to regulators or customers. Another challenge in data quality is the need to manage potential unintended bias in model training data; historical transaction data may reflect enforcement or policy biases that could skew model outcomes.

While AI tools may lower compliance costs over time, adopting and implementing these tools require large upfront costs for financial institutions. These costs may prove prohibitive to smaller financial institutions, particularly those that are unable to dedicate resources to train their own AI systems to replace existing rules-based compliance systems. Financial institutions should also consider the ongoing costs of model maintenance, governance, monitoring, and validation to comply with what may be new and evolving regulatory standards and emerging cybersecurity risks stemming from the use of AI tools.

Financial institutions highlighted that leveraging AI tools was difficult given that existing regulatory frameworks and supervisory processes, although technology-agnostic, were not designed with the capabilities of innovative technologies like AI in mind. There are certain frameworks that take AI/ML model implementation risks into account, such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework, which emphasizes transparency, documentation, and model-risk validation. However, financial institutions may be reticent to use these frameworks without additional regulatory clarity. Several respondents recommended that Treasury specifically endorse that financial institutions align their AI model development and implementation to these risk management frameworks to increase regulatory and supervisory clarity, and as a way to measure the effectiveness of AI models as deployed by financial institutions. This could allow financial institutions to discontinue running legacy rules-based systems alongside machine learning-based models. Discontinuing parallel runs can decrease costs to institutions, decrease the chance for inefficiencies between systems, and decrease the need for investigatory time and resources.

### *Illicit Uses of AI*

AI tools can also be used by adversarial actors. Law enforcement and regulators have warned that criminals can use deepfake media content, such as AI-generated images, video, and documents, to aid in their attempts to perpetrate fraud and bypass customer identification requirements at U.S. financial institutions.[44] Criminals create deepfake images by modifying an authentic source image or creating a synthetic image, and criminals have also combined GenAI images with stolen or fraudulently obtained personally identifiable information (PII) or entirely fake PII to create synthetic identities. According to analysis of BSA data, malicious actors have then successfully opened accounts using fraudulent identities suspected to have been produced with GenAI and used those accounts to receive and launder the proceeds of other fraud schemes. Industry outreach and the RFC highlighted the use of GenAI tools for phishing, deepfakes, and to scan vast repositories of breached or hacked data to find PII, which can be used to make high-quality fraudulent documents and identification.

## Treasury Policy and Efforts

Pursuant to the Executive Order on Removing Barriers to American Leadership in Artificial Intelligence, the Winning the Race America’s AI Action Plan, and the Executive Order on

[44] FinCEN, “Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions,” (November 13, 2024) https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

Ensuring a National Policy Framework for Artificial Intelligence, it is the policy of the United States to sustain and enhance America's global AI dominance.[45,46,47] In line with the Administration's priorities, Treasury has a core objective to advance responsible AI adoption in the financial sector by working with financial institutions, technology partners, and regulators to support innovation and economic growth while safeguarding market integrity, operational resilience, and financial stability. Treasury has also applied AI to improve Treasury operations, deploying AI to enhance the department's analytic capabilities, improve service delivery, and increase the efficiency of the department's programs. Treasury is leading efforts to promote U.S. leadership through global and federal AI alignment by engaging with the interagency and international partners to shape the standards and frameworks that govern AI adoption across financial systems around the world. However, the recommendations below address policy objectives consistent with this report's focus on illicit finance.

In the 2024 National Illicit Finance Strategy, Treasury identified that financial institutions can improve their AML/CFT programs and compliance by leveraging innovative technologies, and that innovations in AI, including machine learning and LLMs, have significant potential to strengthen AML/CFT compliance.[48] In particular, these innovative technologies have the potential to help financial institutions analyze massive amounts of data and more effectively identify illicit finance patterns, risks, trends, and typologies.

Treasury routinely engages with the financial services industry to consider how financial institutions are using AI tools, assess their benefits for AML/CFT compliance, and encourage the responsible use of these tools for compliance purposes. In 2025, Treasury directly engaged with technology firms that are developing advanced LLMs—so-called "frontier model" developers—to understand areas where the technology can be used to combat illicit finance and assist financial institutions' AML/CFT compliance obligations. In addition to this and other engagement, Treasury has researched, sought public comment on, and published a variety of reports on the topic of AI in the financial services sector in recent years. For example, in March 2024, Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) published "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," which was the result of interviews with industry on how financial services, information technology firms, data providers, and anti-fraud and AML companies understand the opportunities and risks of the technology.[49] The report noted that in the past several years, Treasury has leveraged its interagency and public-private partnerships to share information and explore best practices for mitigating the threats that financial institutions face from cybersecurity gaps and vulnerabilities, including in identity processes.

[45] *See* E.O. 14179, 90 FR 8741, https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence.

[46] *See* Winning the Race America's AI Action Plan, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[47] *See* E.O. 14365, 90 FR 58499, https://www.federalregister.gov/documents/2025/12/16/2025-23092/ensuring-a-national-policy-framework-for-artificial-intelligence.

[48] *See* 2024 National Strategy for Combating Terrorist and Other Illicit Financing, May 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf.

[49] Treasury, "U.S. Department of the Treasury Releases Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Sector," March 27, 2024, https://home.treasury.gov/news/press-releases/jy2212.

Treasury has considered these risks carefully, including how deepfake media can be used to defeat customer identification procedures at financial institutions, and how GenAI assists scammers and fraudsters to deploy highly convincing social engineering schemes.[50] As part of efforts to promote the responsible, risk-based adoption of these technologies, Treasury has issued alerts to help financial institutions identify fraud schemes associated with the use of deepfake media created with GenAI tools, explain typologies associated with these schemes, and provide red flag indicators to assist with identifying and reporting related suspicious activity. Based upon its research and industry and law enforcement engagement, Treasury recognizes that GenAI tools hold tremendous potential to assist the government and financial sector in fighting financial crime, while understanding that bad actors seek to exploit the same technology to defraud American businesses and consumers, including financial institutions and their customers.

*Spotlight: NIST AI Risk Management Framework*

In January 2023, the National Institute of Standards and Technology (NIST) published the NIST Artificial Intelligence Risk Management Framework (AI RMF). The AI RMF offers a resource to organizations designing, developing, deploying, or using AI systems to help manage the risks of AI and promote its trustworthy and responsible development and use. Financial institutions participated in NIST's Request for Information process that led to the creation of the AI RMF, and many financial institutions reference the AI RMF in the development and use of AI tools or use the AI RMF to enhance their AI policies, procedures, and controls. NIST's AI RMF helps institutions understand the risks when considering, implementing, and using AI technologies by considering how to govern AI, map its intended purposes and benefits, measure the effectiveness of AI tools through approaches and metrics, and manage risks based on ongoing assessments so that AI systems achieve their intended purpose and objectives.

Given the feedback received from respondents and to support America's global AI dominance, Treasury must take additional steps to foster responsible technological innovation and harness technology to mitigate illicit finance risks and further encourage greater use of AI tools by financial institutions to more effectively and efficiently detect and disrupt illicit finance and promote U.S. leadership.

## Adopted Recommendations

1. Treasury will leverage its public-private partnerships and ongoing dialogues with industry to create venues where financial institutions can share lessons and good practices on leveraging AI tools for AML/CFT compliance, and where Treasury can learn about the further development of these tools to maintain a strong understanding of how

[50] FinCEN, "FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions," November 13, 2024, https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial.

financial institutions are using AI tools for compliance as well as challenges they face in doing so.

2. Treasury will issue guidance, statements of support, or FAQs, as appropriate, to further encourage financial institutions to leverage AI as part of risk-based AML/CFT policies and procedures. Treasury will also explore additional opportunities to support financial institutions leveraging AI to improve compliance and fight financial crime.

3. Treasury, in partnership with NIST, will evaluate opportunities to use NIST's AI Risk Management Framework to inform financial institutions' use of AI/ML tools.

## Section 5: Digital Identity

### Overview

Digital identity verification (also known as "identity proofing") is the process of establishing and verifying that "an attribute or set of attributes uniquely describes a subject within a given context." This includes persons and non-person entities (NPEs).[51] Digital identity can incorporate different attributes, such as biometric data about people, identifiers like addresses for NPEs (e.g., wallets, organizations, devices), and contextual data such as relationships and transactions. Digital identity tools can verify identity evidence such as government-issued identity documents or biometric presentation (e.g., a selfie photo), or inspection of a cryptographic key from a wallet. Tools can vary by operational models, governance, and convenience. Digital identity verification tools can potentially be used by all financial institutions, including DASPs, to support onboarding, automatically check for a credential before executing a user's transaction, and implement other compliance measures.

Identity fraud and theft by illicit actors are a significant threat to the financial sector. Through methods like physical theft, coercion, phishing, data breaches, malware, and other means, illicit actors can use individuals' personal information and physical credentials—either stolen or falsified—to commit a range of financial crimes, such as opening new accounts, making unauthorized transactions, or taking over existing accounts. These identity-related crimes create monetary and reputational losses for customers and financial institutions and enrich illicit actors. As digital assets have been increasingly adopted around the globe, illicit actors have similarly sought to obtain digital assets by circumventing entities' customer identification protocols using fake and stolen personal information and credentials.

### Uses by Financial Institutions

Digital identity has a wide range of practical uses in the financial sector. For regulated digital asset intermediaries, digital identity solutions can support efforts to verify the identities of customers while preserving user privacy. Some tools may use unique capabilities within the digital asset space, with some tokenizing credentials and others tying the credential to a digital asset wallet address and preventing transfers to other addresses. In response to Treasury's RFC,

[51] NIST, "Glossary: Digital Identity," https://csrc.nist.gov/glossary/term/digital_identity; NIST, "Glossary: Non-person Entity (NPE)," https://csrc.nist.gov/glossary/term/non_person_entity.

digital asset industry leaders and advocacy groups endorsed the further development of digital identity due to its innovative potential for countering illicit finance involving digital assets, streamlining compliance requirements, and maintaining privacy for customers. Approximately half of RFC respondents raised digital identity.

A large variety of digital identity tools and applications currently exist, and there are a significant number under development. In certain cases, digital credentials are issued based on physical attributes, such as requiring a credential recipient to appear in person or requiring physical documents for collection and verification prior to issuance of a credential. In light of the development of mobile driver's licenses (mDLs), a form of state-issued digital identity that is equivalent to a physical ID[52] and compliant with REAL ID and other national standards, financial institutions may turn to using mDLs to help satisfy customer due diligence and identification requirements.

Digital identity includes portable digital identity solutions, whereby financial institutions that have conducted customer identification and verification may issue credentials that can be held by a financial institution or individual and then shared with other financial institutions for customer due diligence purposes. These tools can be queried for the specific information required on a "need-to-know" basis, which can then be layered into a customer's risk score. In some cases, these credentials can also incorporate cryptographic tools such as "zero-knowledge proofs," which enable a person to prove that they are who they claim to be without revealing information other than that fact. The information contained in these credentials can be updated on a dynamic basis if identifiers change, and the nature of the cryptography used often means that illicit actors cannot reengineer an identity, even if they use AI. The more diffuse nature of this type of digital identity may also create fewer large identity targets for illicit actors to exploit. While portable tools have the potential to streamline compliance without over-collecting information, they are still not widespread.

These types of verifiable credentials represent innovative means for financial institutions, including DASPs, to conduct customer identification and verification while minimizing the amount of sensitive data collected. While the applicability of each of these tools varies, they offer a potential pathway to support intermediaries' ability to mitigate identity fraud and other sources of identity-related illicit finance risk mitigation in the digital asset ecosystem.

Foreign counterparts are also prioritizing the development of digital identity to assist the financial sector in streamlining compliance. For example, in 2024, the European Union's (EU) eIDAS 2.0 regulation established a framework for electronic identification, authentication, and trust services, including the European Digital Identity Wallet, which EU member states must provide to citizens by late 2026. The EU is requiring acceptance of this digital identity by financial institutions such as banks and DASPs by late 2027 to bolster secure, cross-border onboarding and to streamline customer due diligence.[53] The United Kingdom is also supporting digital identity through new legislation, which places digital identity standards on a statutory

[52] mDLs digitally replicate the data and security of physical IDs through cryptography and biometric verification that enables real-time validation.

[53] European Commission, "European Digital Identity," https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en.

footing, and through upcoming guidance around its AML regulations to recognize the use of digital identity for streamlined customer onboarding, fraud reduction, and better data privacy.[54]

As part of the RFC, industry shared that financial institutions and third-party vendors seek to leverage and promote the use of digital identity tools to:

- Reduce the risks of onboarding fraudulent customers;
- Improve customers' experience by reducing friction in onboarding;
- Prevent unauthorized access to legitimate accounts by illicit actors;
- Augment existing customer identification programs (CIP) or even replace physical credentials for some customers;
- Protect customers' private information; and
- Reduce long-term compliance costs and burdens, among others.

Digital identity systems can be protected through the use of encryption, multi-factor authentication, continuous monitoring, and attack detection tools, as well as by adhering to rigorous standards for assurance, such as those outlined by NIST.[55] For instance, digital identity can be used to protect sensitive digital asset trades via mutual authentication mechanisms or "transaction signing" with a passkey-enabled credential. Integrating liveness detection, which is a technology that can detect presentation attacks (i.e., to determine if a biometric sample such as a face is from a living person instead of a photo, mask, or deepfake), into digital identity tools can close loopholes in legacy systems that are exploited by illicit actors. Issuers of digital identity can also maintain revocation mechanisms to invalidate compromised credentials.

When considering whether to adopt digital identity tools, third-party vendors and regulated financial institutions highlighted that they considered a variety of factors including: the alignment of the tool with NIST and other international standards; the level of assurance (the rate at which a tool can accurately verify a person is who they claim to be) provided by the tool; data security; user experience and likelihood of adoption by customers; auditability of the tool by regulators; and cost. Based on feedback to Treasury's RFC, additional considerations include regulatory acceptance and each institution's risk profile, with institutions dealing with high-risk, cross-border customers engaged in digital services more likely to adopt digital identity tools. Developers posit that financial institutions' up-front costs of adopting digital identity may be offset over time by gains from automation and reductions in fraud losses.

In the case of innovative digital identity tools provided by trusted third-party issuers, industry respondents noted that government and law enforcement authorities can benefit from verifiable, tamper-evident audit trails tied to cryptographic proofs that can allow authorities to more easily query identifiers and ascertain linkages between a specific person and illicit activity. Commenters also highlighted the utility of digital identity in the DeFi ecosystem, including potentially the ability for smart contracts to automatically check for a credential before executing a user's transaction and the technical ability of tools, subject to appropriate use, that incorporate

[54] UK Office for Digital Identities & Attributes, "Trusted digital identities in financial services: new MLR guidance announced," July 23, 2025, https://enablingdigitalidentity.blog.gov.uk/2025/07/23/trusted-digital-identities-in-financial-services-new-mlr-guidance-announced/.
[55] *See* NIST, Digital Identity Guidelines, NIST SP 800-63 Digital Identity Guidelines.

a user's transaction history on the public blockchain into their identity profile, thereby providing additional information to digital asset intermediaries and other counterparties on a user's behavior and exposure to illicit finance risks.

*Challenges*

However, there are several key obstacles to the adoption of digital identity by financial institutions. Multiple respondents, including both financial institutions and third-party service providers, highlighted a need for more specific guidance around the acceptance of digital identity as an allowable form of identification for financial institutions' customer identification programs in order to enable adoption, especially when leveraging digital identity tools in lieu of collecting copies of physical identity documents. In addition to the need for guidance or a statement from regulators, respondents also noted ongoing concerns with supervisory approaches and the risk of negative feedback from bank examiners regarding the use of these tools.

Another key challenge identified by industry is the level to which specific verified credentials are accepted across different platforms domestically and internationally, which is especially important in the context of cross-border digital asset transfers. Similarly, fragmentation between federal, state, and other digital identity initiatives and standards highlights the need for national alignment. Interoperability between different digital identities also remains a challenge. In addition, many financial institutions are running legacy systems that may require significant, costly upgrades in order to integrate digital identity tools. Cost barriers may be especially salient for smaller institutions, as well as state and local authorities, in the absence of additional funding.

Respondents also highlighted the risk that the development of digital identity solutions, depending on how the tools function, could create large repositories of customers' PII, which would pose a prime target for cybercriminals. Recent breaches of customer PII across the financial services industry offer examples of how this might occur in practice. However, legacy processes at financial institutions that overly rely on physical identification in lieu of more targeted, secure digital identity tools also pose risks of breaches and, as some in industry contend, may pose even higher risks.

Finally, members of the public expressed opposition to customer identification requirements, including those that leverage digital identity, for DeFi due to perceived risks to individual privacy and the innovative nature of the DeFi ecosystem. At the same time, some entities support the development of privacy-preserving digital identity tools to meet countering illicit finance objectives within certain parts of the DeFi ecosystem, outside of any potential BSA obligations.

## Treasury Policy and Efforts

Treasury recognizes that digital identity tools can be leveraged for customer identification and verification by all types of financial institutions to combat the growth of identity fraud. Certain digital identity solutions can also be uniquely useful in a blockchain-based system where tokenized credentials can be embedded in smart contracts. As part of its overall stance of supporting innovation, Treasury will support efforts by financial institutions to create and adopt digital identity solutions, including in the DASP sector, to protect customers and cut down on illicit financial flows.

Leveraging new technologies to combat identity fraud is an urgent need, given Treasury's analysis of a significant number of identity-related exploitations and illicit identity-related schemes. For instance, FinCEN found that in 2021, approximately 1.6 million BSA reports (42 percent of reports filed that year) related to identity, indicating $212 billion in suspicious activity.[56] FinCEN identified over 14 typologies commonly indicated in identity-related BSA reports, of which the most cited typologies included fraud, false records, identity theft, third-party money laundering, and circumvention of verification standards. In particular, FinCEN found that compromised credentials have a disproportionate financial impact as compared to other types of identity exploitation.[57]

To promote the use of digital identity solutions, including for the purpose of combating identity fraud, Treasury maintains an ongoing collaboration with NIST and other interagency partners to identify and promote emerging approaches to digital identity. Treasury in 2025 provided support to NIST in its publication of the fourth revision of its Digital Identity Guidelines, which are a set of technical requirements for federal agencies to implement secure digital identity tools. The guidelines cover issues such as identity proofing, registration, authentication, and identity assurance levels, as well as new guidance on passkeys, digital wallets, and deepfakes.[58] Many private sector entities also use these guidelines as a standard against which they can assess the effectiveness of digital identity tools. Treasury is working with NIST to understand lessons learned from their ongoing pilot with financial institutions related to the use of mDLs.

In addition, Treasury has been exploring how digital identity can be leveraged by financial institutions, including to counter illicit finance, through collaboration with public and private sector partners. For example, in 2022, FinCEN and the Federal Deposit Insurance Corporation (FDIC) hosted a Digital Identity Tech Sprint, in which eight teams of participants demonstrated their solutions to an expert evaluation panel.[59] As part of this event, FinCEN and the FDIC focused teams on helping measure the effectiveness of digital identity proofing, which is the first step in the creation and use of digital identity credentials.

Treasury has worked within international standards-setting bodies such as the FATF to assist governments and financial institutions in determining if a digital identity system is trustworthy and reliable. The FATF published in 2020 its Guidance on Digital Identity, a project which was co-led by Treasury and is designed to help government authorities and financial institutions use digital identity tools to conduct customer due diligence in a risk-based manner.[60] The guidance

[56] FinCEN, "Financial Trend Analysis: Identity-related Suspicious Activity: 2021 Threats and Trends," January 2024, https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf.

[57] FinCEN, "Financial Trend Analysis: Identity-related Suspicious Activity: 2021 Threats and Trends," January 2024, https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf.

[58] NIST, "Special Publication 800-63-4: Digital Identity Guidelines," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf.

[59] *See* FDIC FinCEN Digital Identity Tech Sprint – Key Takeaways and Solution Summaries, September 9, 2022, https://www.fincen.gov/news/news-releases/fdic-fincen-digital-identity-tech-sprint-key-takeaways-and-solution-summaries.

[60] *See* FATF Guidance on Digital ID, March 6, 2020, https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html.

aims to make financial services more secure, efficient, and accessible. It outlines the benefits and risks of using digital identity tools and discusses how to determine a system's level of assurance.

The Treasury Department recognizes that digital identity solutions, including tokenized credentials, will help financial institutions combat fraud. Empowering financial institutions to further leverage tokenized credentials and reliance within customer identity programs will reduce redundancy and burden, key goals of the Administration's efforts to reduce regulatory burdens. At the same time, small to mid-size financial institutions and businesses may face resource constraints in upgrading technology to enable the acceptance of digital identity solutions. Treasury should work with banks of all sizes, including community banks, to identify potential resources needed to leverage innovative tools.

### Adopted Recommendations

1. Treasury will issue guidance to financial institutions on how they can utilize verifiable digital credentials consistent with their existing customer identification programs.[61]

2. Treasury will explore working with Congress on legislation to incentivize the development and integration of digital identity tools aimed at countering illicit finance, such as providing additional grant funding, particularly for small businesses and state authorities.

3. Treasury, in consultation with NIST, will work with international partners to promote common guidelines regarding the use of digital identity tools to counter illicit finance by financial institutions and DASPs, with the goal of bolstering interoperability across jurisdictions.

4. Treasury will explore working with Congress on ways to better enable third-party service providers to conduct identity verifications and issue verifiable digital credentials that can be accepted by financial institutions to fulfill elements of customer identification and verification requirements.

## Section 6: Blockchain Monitoring and Analytics

### Overview

Blockchain monitoring refers to the process of observing, tracking, and analyzing public blockchain data. The U.S. government, like many financial institutions offering services in

[61] Customer Identification Program requirements were jointly issued in 2002 by the Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA) to implement section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. See 31 CFR 1020.220 (FinCEN); 12 CFR 21.21(c)(2) (OCC); 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(j)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); and 12 CFR 748.2(b)(2) (NCUA). There are other Customer Identification Program regulations for other types of financial institutions, such as broker-dealers and mutual funds.

digital assets, leverages public blockchain data and blockchain analytics to trace and attribute illicit activity in digital assets. Financial institutions can also use this data to evaluate high-risk counterparties and activities, analyze transactions across multiple blockchains, trace or monitor transaction activities, and identify patterns that indicate potential illicit transactions.

## Uses by Financial Institutions

Treasury received 65 comments that discussed blockchain technology and monitoring in response to the RFC. Commenters broadly agreed that financial institutions with substantial exposure to digital assets have already incorporated blockchain analytics tools into their AML/CFT and sanctions compliance programs. These tools enable financial institutions to monitor blockchain activity, identify suspicious or unusual transaction patterns, and conduct due diligence. Blockchain monitoring tools also enable financial institutions to screen transactions for suspected illicit activity.

Commercially available blockchain analytics tools often incorporate a range of features and proprietary data and techniques to support financial institutions' AML/CFT and sanctions compliance programs. Core features of compliance-oriented blockchain analytics tools include address attribution and clustering, transaction tracing and monitoring, and counterparty risk scoring. In addition to attributing specific addresses or address clusters to illicit or high-risk actors, blockchain analytics tools can detect transactional patterns associated with potentially suspicious activity, such as peel chains.[62] Compliance solutions frequently integrate blockchain data with off-chain data. This off-chain data thread can include threat intelligence, PII and entity attribution data, IP address and device data, and open-source intelligence.

Additional blockchain analytics capabilities that commenters described include:

- Use of AI algorithms to conduct sophisticated analysis of blockchain data and reduce false positives;
- Detecting potentially malicious blockchain activity, such as code changes and malicious smart contract deployments;
- Ensure Travel Rule[63] compliance;
- Detecting address poisoning;[64]
- Provide platforms for sharing threat intelligence among verified participants;

[62] Peel chains occur when a large amount of cryptocurrency sitting at one address is sent through a series of transactions in which a slightly smaller amount is transferred to a new address each time. In each transaction, some quantity of cryptocurrency "peels off" the chain to another address—frequently to be deposited into a virtual currency exchange—and the remaining balance is transferred to the next address in the chain.

[63] To the extent that any money transmitter's transactions constitute a "transmittal of funds" under FinCEN's regulations, then the money transmitter must comply with the "Funds Transfer Rule" or "Travel Rule." Under the rule, a transmittal of funds of $3,000 or more may trigger certain requirements on a DASP such as an exchange that constitute a money transmitter acting as either a financial institution for the sender or receiver of the transfer, or as an intermediary financial institution. For example, it may require a DASP to collect, verify, and share sender and receiver information for digital asset transactions at or over the specified amount.

[64] Address poisoning occurs when an adversary first generates lookalike addresses similar to one with which the victim has previously interacted and then engages with the victim to "poison" their transaction history. The goal is to have the victim mistakenly send tokens to the lookalike address, as opposed to the intended recipient.

- Deploy scripting capabilities;[65]
- Trace transactions across cross-chain bridges;[66]
- Deploy heuristics[67] and visualizations;
- Integrate APIs that support integration with external data sources or integration with existing compliance functions; and
- Deploy smart contract tracking.[68]

Feedback from industry emphasized that financial institutions use blockchain analytics as a supplement to, rather than a replacement for, other AML/CFT and sanctions compliance tools. Blockchain analytics platforms often rely on probabilistic heuristics to draw conclusions, and may have gaps in their coverage of addresses, assets, and blockchains. In addition, obfuscation tools such as mixers and the use of anonymity-enhanced digital assets can complicate blockchain tracing. Illicit actors also switch between services and blockchains to obfuscate transaction flows. Some analytics tools offer the capability to trace transactions across chains, but this requires complex heuristics and is likely to reduce confidence in the conclusion of the analysis.

Industry highlighted that there are also roadblocks for financial institutions seeking to implement blockchain analytics tools, including potential regulatory ambiguity and cost. Financial institutions, according to respondents, face uncertainty regarding how examiners will assess their use of blockchain analytics as part of their AML/CFT and sanctions compliance programs, especially because examiners need expertise in blockchain tools to evaluate the adequacy of financial institutions' controls. In addition, implementing blockchain analytics tools can be cost-prohibitive for smaller institutions due to the expense of procuring the technology, integrating the platform with the financial institution's other systems, and hiring or training expert staff.

A lack of common technical standards for conducting blockchain analytics also presents a challenge for financial institutions in evaluating vendors and developing best practices. Blockchain analytics tools frequently use proprietary heuristics, such as cluster analysis, to reach conclusions. This leads some financial institutions to use multiple tools to corroborate the conclusions of blockchain analytics. In addition, there are no uniform standards for recording and presenting evidence derived from blockchain analytics. This leads financial institutions to rely on imperfect methods, such as saving screenshots. Feedback from industry also highlighted that the lack of standardization, combined with reliance on proprietary data, can complicate the sharing of illicit finance-related information among financial institutions and blockchain analytics firms.

[65] For those performing blockchain analysis, scripting refers to the use of programming languages and tools to analyze data stored on the blockchain. These tools, which could be custom-built, can interact with and interpret the available data to assist pattern identification.

[66] Cross-chain bridges allow users to exchange digital assets or information from one blockchain to another.

[67] Heuristics are data-driven rules that help investigators ascertain relationships between digital asset addresses and cluster them to identify persons, trace funds, and spot illicit activity through a set of assumptions about transaction patterns.

[68] Smart contract tracking is the process of monitoring, analyzing, and verifying the execution of self-executing digital agreements (smart contracts) on a blockchain by using tools to gain insights into their automated processes and flows.

## Treasury Policy and Efforts

Treasury recognizes that blockchain monitoring and other analytics tools can contribute to financial institutions' ability to counter illicit finance. In developing guidance, advisories, and other publications, Treasury includes material relevant to financial institutions using blockchain analytics tools, where appropriate. For example, FinCEN has published several advisories, alerts, and notices that contain red flag indicators for financial institutions using blockchain analytics.[69] In 2018, OFAC began including digital asset addresses as identifying information for persons listed on the Specially Designated Nationals and Blocked Persons (SDN) List. In 2021, OFAC published a compliance brochure for the digital asset industry, which included information on the use of transaction monitoring and investigation software as part of a sanctions compliance program.[70] OFAC also published several FAQs related to digital assets.[71] OFAC does not require companies to use any specific tool for sanctions screening, but it has recognized companies' implementation of compliance programs and use of blockchain tracing as a mitigating factor in enforcement actions.[72] FinCEN has also recognized the utility of blockchain analytics tools, where appropriate, as part of a risk-based AML program, and has highlighted gaps in AML/CFT compliance in certain enforcement actions where financial institutions had not leveraged such tools.[73]

Treasury's research and analysis in response to the RFC also identified the wide array of innovative AML/CFT compliance solutions built on blockchain technology. Because of the diversity of industry approaches to blockchain-based products, it is important for Treasury to maintain a technology-neutral approach to regulation that empowers financial institutions to use the tools that best support their risk-based compliance programs. In addition, because any given AML/CFT compliance tool is only one part of a financial institution's overall AML/CFT program, Treasury seeks to avoid excessively prescriptive approaches to mitigating illicit finance risk in the digital assets ecosystem. Favoring one technology, rather than encouraging institutions to leverage innovative tools as part of a risk-based approach, could deter financial institutions' effective use of multiple tools.

Treasury also recognizes that it has an important role to play in bringing together public and private sector stakeholders to address the unique illicit finance issues facing the digital assets ecosystem. For example, in August 2025, FinCEN brought together Treasury components, law

[69] *See, e.g.*, FinCEN, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019); FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (November 8, 2021); FinCEN, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering'" (September 8, 2023); FinCEN "FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity" (August 4, 2025); and FinCEN, "FinCEN Notice on Financially Motivated Sextortion" (September 8, 2025).

[70] *See,* OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry, October 2021, https://ofac.treasury.gov/media/913571/download?inline.

[71] *See,* https://ofac.treasury.gov/faqs/562, https://ofac.treasury.gov/faqs/563, https://ofac.treasury.gov/faqs/594.

[72] *See*, *e.g.*, OFAC, "OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs" (October 11, 2022).

[73] *See,* FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act | FinCEN.gov; FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act | FinCEN.gov; FinCEN Announces Largest Settlement in U.S. Treasury Department History with Virtual Asset Exchange Binance for Violations of U.S. Anti-Money Laundering Laws | FinCEN.gov.

enforcement agencies, financial institutions, regulatory technology companies, and trade groups to share insights on driving innovation in the digital assets ecosystem while protecting consumers from emerging fraud and scam threats.[74] Treasury will continue these engagements and seek opportunities to build consensus among public and private sector partners in order to address major illicit finance threats, facilitate cooperation and information-sharing, and encourage alignment around common best practices and technical standards.

Feedback from public comments made clear that, although blockchain monitoring tools have become essential components of AML/CFT compliance programs, gaps, inconsistencies, and barriers to effective use still exist. Treasury's assessment of this feedback highlighted several interconnected requests: 1) clearer supervisory expectations; 2) improved examiner expertise; 3) greater consistency in technical and evidentiary standards; and 4) stronger mechanisms for information-sharing across the financial sector. Treasury's analysis of the comments further suggests that smaller-sized institutions are inhibited by operational and cost challenges in adopting and integrating blockchain analytics, and that these challenges are compounded by perceived regulatory uncertainty and limited industry standardization.

In evaluating these themes, Treasury has identified opportunities where targeted support, public-private engagement, and policy development could strengthen the overall effectiveness of blockchain analytics within risk-based AML/CFT compliance programs. This assessment directly informed the subsequent recommendations, such as focusing on enhancing supervisory capacity, facilitating broader sharing of illicit finance insights, advancing the development of best practices and technical standards, and exploring legal tools that enable institutions to respond more effectively to suspected illicit activity.

## Recommendations

1. Treasury will engage with industry to understand best practices and technical requirements for implementing blockchain analytics tools in AML/CFT compliance.

2. Treasury will support financial supervisors' efforts to evaluate whether additional AML/CFT and sanctions compliance tools, training, and internal resources are needed to ensure examiners can effectively and efficiently evaluate institutions' digital asset-related internal policies, procedures, and controls, including how those attributes leverage blockchain analytics.

3. Treasury will promote greater sharing of blockchain-related illicit finance insights and indicators between and among financial institutions and blockchain analytics firms.

4. Treasury will explore working with Congress to potentially incorporate legislative amendments to clarify and/or update the framework for voluntary information sharing among financial institutions, including the permissibility of sharing in relation to fraud detection and prevention.

[74] FinCEN, "FinCEN Convenes Public-Private Partnership to Promote Innovation and Address Fraud and Scam Risks in the Digital Assets Ecosystem," https://www.fincen.gov/news/news-releases/readout-fincen-convenes-public-private-partnership-promote-innovation-and.

5. Congress should consider enacting a digital asset-specific “hold law” that offers a safe harbor to institutions that temporarily and voluntarily hold digital assets involved in suspected illegal activity during a short-duration investigation. Such a law should consider transparency when an asset is frozen and consumer protection measures. Such a law would be particularly useful for countering illicit finance involving permitted payment stablecoins.

6. Treasury will explore enhancing the ability of institutions to leverage technologies as part of its information-sharing authorities, including section 314(b).

## Section 7: Application Programming Interfaces

### Overview

APIs are a system access point or library function that allows different software applications to communicate and interact with each other, including internal and external applications.[75] This can include various applications used by a financial institution for AML/CFT and sanctions compliance. APIs can be used to share data automatically and facilitate access to transaction information. Once deployed, they can also be used to help enforce strict access controls, monitor transactions and activities, and bolster the security and integrity of financial institutions providing digital asset services.

### Uses by Financial Institutions

In response to the RFC, Treasury received extensive feedback on the use of APIs from more than 50 respondents, ranging from major financial institutions to trade associations, technology providers, blockchain analytics firms, DASPs, and individual subject matter experts. The majority of respondents expressed strong support for the expanded use of APIs to enhance the speed, security, and interoperability of compliance systems for AML/CFT efforts. A smaller subset raised concerns regarding privacy, cybersecurity, and the potential overreach of API-based data sharing. Overall, respondents reported that APIs function as a core emerging technology in support of innovatively detecting illicit activity in the digital asset ecosystem.

Industry characterized APIs as foundational technologies that enable secure, real-time communication between disparate systems within and across institutions. APIs are viewed as critical to integrating compliance functions across fiat and blockchain ecosystems—enabling seamless information flow that supports sanctions screening, transaction monitoring, and CIP. To that end, APIs may serve as the connective tissue of modern compliance frameworks, automating CIP, risk scoring, and suspicious activity monitoring while reducing manual effort and latency.

Respondents highlighted the role of standardized APIs in establishing cohesive compliance ecosystems. APIs connect into AML/CFT systems, blockchain analytics platforms, and digital identity verification services—creating real-time decisioning processes that operate across

[75] NIST, “Securing Web Transactions TLS Server Certificate Management” (June 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf, pg. 54.

networks and jurisdictions. APIs further facilitate pre-transaction risk assessments—improving the likelihood that illicit transfers can be intercepted before settlement—which is an essential function in the context of analyzing digital asset tools' interdiction efforts.

### *Challenges*

Industry has acknowledged that API adoption, while beneficial, introduces significant operational and financial burdens—indicating that implementation requires specialized technical expertise, ongoing maintenance, and integration with legacy systems that may not support modern frameworks. Smaller institutions have signaled that these demands could exacerbate resource disparities between small and large firms within the financial services sector. A significant risk attributed to the proliferation of inconsistent API standards and vendor dependencies is compounding integration costs; promoting standardized and open-source API specifications to reduce complexity and improve scalability could further attenuate outsized integration costs.

Concerns regarding privacy, cybersecurity, and data governance were prevalent across responses. APIs expand potential attack surfaces by introducing new data transmission points and increasing exposure to unauthorized access. Thus, it is imperative to stress the importance of adopting robust encryption protocols, mutual Transport Layer Security, and strict access controls to safeguard sensitive financial and personal data.

Commenters stated there is a significant policy and operational challenge to wider API adoption, which can be characterized by the misalignment between automated API-driven compliance capabilities and existing BSA obligations and examiner familiarity. Presently, there are no standardized agreements and liability frameworks that govern relationships between payment networks, issuing banks, and merchants—making it challenging to demonstrate that clear, interoperable trust arrangements can balance compliance assurance with operational scalability. Further, the BSA does not give examiners guidance on recognizing API-based attribute-level attestations as compliant for different required processes. Commenters believed this is principally reflected by the mismatched integration of automated and real-time API processes with BSA requirements that were structurally designed around manual rules and post-facto verification standards. Furthermore, expertise varies widely in reference to familiarity with API-based systems. This can create inconsistent expectations around auditability, traceability, and the evidentiary standards needed to demonstrate compliance. Smaller institutions have additionally signaled challenges in securing vendor support and developing technical capacity.

### *Opportunities*

There is widespread agreement across financial institutions that suggests APIs enhance the ability of financial institutions to detect and prevent illicit finance. APIs enable real-time transaction monitoring, sanctions screening, and automated reporting, transforming compliance from reactive processes into proactive control mechanisms. These tools support dynamic risk management by integrating blockchain data and data on fiat currency movements, improving response times, and reducing false positives through automation and data enrichment.

The applied capabilities of APIs have reflected measurable gains in efficiency, interoperability, and accuracy across compliance systems. Respondents credited APIs with improving data sharing between institutions, enhancing automation, and lowering compliance costs through reusable credential validation. Institutions indicated that API-driven solutions align closely with the GENIUS Act research factors by improving detection accuracy, operational efficiency, and privacy while reducing the overall sensitivity and volume of data exchanged.

## Treasury Policy and Efforts

Treasury has pioneered several technical efforts to advance the use of APIs as a way to: (1) enhance data accessibility; (2) enable regulatory compliance with government e-filing systems; and (3) facilitate public transparency. Treasury's ongoing modernization efforts reflect a broader commitment to harness secure systems and streamline the exchange of machine-readable data across government and non-governmental platforms.

OFAC has established the Sanctions List Service (SLS), a machine-readable data platform that supports API-based retrieval of sanctions information.[76] The SLS provides financial institutions and the public with structured data feeds, enabling the automatic ingestion of sanctions lists and real-time updates. OFAC is leveraging APIs to facilitate the increased automation of sanctions screening processes across the traditional finance and digital asset ecosystems.

The Bureau of the Fiscal Service maintains the Fiscal Data platform, which hosts an API based on Representational State Transfer architectural principles, colloquially known as "RESTful," and provisions access to official Treasury datasets.[77] This system supports programmatic access to financial data—such as federal debt, auctions, and payments—using standardized APIs.

Given the centrality of APIs to share data across an institution's AML/CFT compliance program, Treasury will seek to promote the use of APIs in a safe and secure fashion. To achieve this, Treasury will work with the interagency to develop standards for the use of APIs. API standards can also assist small and mid-size financial institutions in assessing third-party vendors for APIs, supporting innovative technologies that can be leveraged by all financial institutions.

Treasury's review of industry feedback revealed broad consensus that APIs are an instrumental tool in modern AML/CFT compliance frameworks; however, respondents frequently indicated that their adoption is constrained by inconsistent standards and misalignment with the contours of existing BSA requirements. Industry emphasized that APIs significantly enhance detection accuracy, interoperability, and real-time risk management, yet also highlighted operational burdens, privacy and cybersecurity concerns, and the need for examiners to better understand API-driven systems. This feedback clarified that the innovative benefits of APIs cannot sufficiently be deployed unless institutions have access to scalable, secure, and standardized approaches that reduce integration costs and establish consistent oversight.

Treasury identified actions that reflect its commitment to supporting secure, interoperable, and innovative API deployment across institutions of all sizes. The recommendations below focus on fostering common technical standards, leveraging public-private coordination, and reducing

[76] *See,* OFAC, "Sanctions List Service," https://ofac.treasury.gov/sanctions-list-service. .
[77] *See,* Treasury, Fiscal Data, "API Documentation," https://fiscaldata.treasury.gov/api-documentation/.

barriers to implementation of API-driven compliance tools. These insights emphasize the critical alignment between refining regulatory expectations with the adoption of innovative capabilities and promulgating shared standards that stem from strengthening security and interoperability to facilitate scalable integration across the financial services sector.

### Adopted Recommendations

1. Treasury will leverage its public-private partnerships to create a venue where financial institutions can share lessons and good practices on leveraging APIs.

    a. As part of this effort, Treasury will engage in conversations about how to reduce disparities in technical capacity and resources to adopt advanced compliance tools.

2. Treasury will collaborate with NIST to promote the development and use of standardized and open-source API guidelines.

3. Treasury will encourage industry stakeholders to develop open-source and standardized APIs for essential compliance functions—reducing obstacles for smaller credit unions, community banks, and non-bank financial institutions to adopt, as well as encouraging the development of APIs with robust encryption protocols and strict access controls to safeguard sensitive financial and personal data.

## Section 8: Decentralized Finance

As part of the GENIUS Act, Congress directed Treasury to report on "legislative recommendations relating to the scope of the term 'digital asset service provider' and the application of that term to decentralized finance."[78] Illicit actors leveraging digital assets often use a variety of different methods in the laundering process, including the use of DeFi services. For example, as illustrated in the October 2025 Multilateral Sanctions Monitoring Team Report, DPRK cyber actors have been observed using DeFi services, including decentralized exchanges, bridges, and mixers, to obfuscate the source of stolen funds and evade tracking by regulators and law enforcement.[79] Treasury and industry, however, also recognize that some tools can provide insight into transactions occurring in the DeFi ecosystem.[80] Notably, public and private sector stakeholders may be able to trace digital assets' movement through DeFi services on the public blockchain.

As described further below, Treasury has been considering how to address illicit finance risks in the DeFi ecosystem. While the BSA framework generally treats entities that may fall within the definition of digital asset service providers as MSBs, the current framework does not fully

[78] Section 9(e)(1)(E) of the GENIUS Act.

[79] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," pg. 42-43, https://msmt.info/Publications/detail/MSMT%20Report/4221. The MSMT report found that DPRK cyber actors commonly use some combination of a nine-step process to launder stolen cryptocurrency.

[80] As noted on pg. 23-24 of this report, financial institutions can use blockchain analytics to conduct smart contract tracking and other activities that can deliver valuable insights into transactions occurring in the DeFi ecosystem.

account for certain types of decentralized protocols, such as when the governance or decision-making is distributed across communities of users and the protocols may be immutable. The PWG Report recommended that Congress consider a principled approach to defining various actors in the DeFi ecosystem to provide clarity to industry and allow tailored solutions to mitigate illicit finance risks.[81] Such an approach could include providing direction to the appropriate regulators to clarify how obligations apply to entities that utilize smart contracts or have some characteristics of DeFi but do not meet all elements of a decentralized protocol. As part of this effort, Congress should consider codifying language explicitly setting out which actors, if any, in the DeFi ecosystem may be subject to AML/CFT obligations, taking into consideration those actors' roles in the ecosystem and attendant risks. Depending on the definition, entities subject to such a mandate could include services that have centralized governance, including through instances in which governance tokens are held by one or a small group of persons that can effectively assert control. This could respond to industry's desire for regulatory clarity regarding the permissibility of interacting with non-custodial digital asset services, including DeFi protocols.

In considering statutory changes, Congress should consider the practices that some participants in the DeFi ecosystem are implementing in light of innovative capabilities and focus on which entities are best positioned to mitigate illicit finance risk. Technological capabilities of DeFi ecosystem participants could provide opportunities to use new types of information and tools to mitigate illicit finance, as well as the limitations to implementing the full suite of AML/CFT obligations that generally apply to financial institutions. In terms of technological capabilities, the ability for blockchains, DeFi protocols, and DeFi applications to use blockchain information through oracles or APIs to identify potentially illicit activity may help reduce the ease with which illicit actors are able to leverage DeFi services. Finally, the use of on-chain digital identity and other credentialing frameworks by DeFi services could be useful for risk mitigation and interdiction of illicit activity. Other parts of the ecosystem, such as certain application layer participants, relayers, and remote procedure call (RPC) nodes, are currently implementing risk mitigation measures, including risk-rating wallets and rejecting transactions above a certain risk score. Upon congressional action, Treasury would implement by applying specified obligations to actors in the DeFi ecosystem based on the role that they play and the attendant risks.

As Congress considers what, if any, aspects of the DeFi ecosystem should have AML/CFT obligations, it should consider the following recommendations.

## Recommendations

1. Congress should consider specifying actors within the decentralized finance ecosystem that should be subject to AML/CFT obligations, taking into consideration those actors' roles in the ecosystem and attendant risks.

2. Congress should consider how to best safeguard the U.S. financial system from money laundering threats that originate abroad, including those in the decentralized finance ecosystem. Such steps should include adding a sixth special measure to

[81] "Strengthening American Leadership in Digital Financial Technology," https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, pg. 106-107.

Section 311 authorizing Treasury to prohibit, or impose conditions upon, certain "transmittals of funds" that are not tied to a correspondent banking relationship.

3. Congress should consider creating digital asset-specific financial institution types or subtypes within the BSA, such that the new types or subtypes would be subject to AML/CFT obligations. Pending additional market structure legislation being considered by Congress, FinCEN should evaluate whether and how its existing guidance related to the digital asset sector, including guidance issued in 2013 and 2019, should be rescinded, modified, or updated to reflect legislative and regulatory changes.

    a. As part of this effort, FinCEN could consider whether additional guidance would be appropriate for particular market segments or for the application of particular BSA obligations.

THE DEPARTMENT OF THE TREASURY

1789