Cooley

Treasury DeFi Report Offers Insight Into BSA Compliance

May 9, 2023

Editor's note: Authored by Sean Ruff, Adam Fleisher and Obrea Poindexter, this article was originally published in Law360.

After a period of rapid innovation and growth in the virtual currency and digital asset space, state and federal regulators have recently issued statements, guidance and reports that articulate specific concerns and corresponding regulatory expectations with respect to digital asset activities.

Case in point is the recent "Illicit Finance Risk Assessment of Decentralized Finance"[1] released by the U.S. Department of the Treasury last month.

This report, which is part of the Treasury's recent investigations of digital assets as required by the 2022 executive order on digital assets,[2] reaffirms that the Treasury Department sees significant risks associated with decentralized finance, or DeFi, services and the potential impact on efforts to combat money laundering and terrorist financing.

The new report follows the Treasury's March 2022 "National Money Laundering Risk Assessment,"[3] which first identified DeFi as an illicit finance risk.

That money laundering risk assessment briefly identified illicit finance risks associated with DeFi, noting that "[c]riminals and professional money launderers continue to use a wide variety of methods and techniques, including traditional ones, to place, move, and attempt to conceal illicit proceeds ... [including] the ever-evolving world of virtual assets and related service providers, including decentralized finance and the growing use of anonymity-enhancement technologies."[4]

Unlike the previous risk assessment, however, this new report is focused not only on money laundering and illicit finance risk, but also on addressing the regulation of DeFi activities under the existing Bank Secrecy Act regulatory regime, particularly as applied to money services businesses, or MSBs.

The report's statements regarding vulnerabilities due to the uncertain and inconsistent application of the BSA should be of significant interest to industry participants that may have been waiting for additional guidance regarding whether and to what extent the BSA applies to new and innovative services in the DeFi space.

Regulation of Virtual Currency Activities Under the BSA

The Bank Secrecy Act imposes anti-money laundering, or AML, and countering the financing of terrorism, or CFT, obligations on financial institutions such as banks, broker-dealers and MSBs, which include companies that provide money transmission services — a broad category encompassing significant amounts of fintech and virtual currency activity.

A covered financial institution subject to AML/CFT compliance program obligations must establish and implement an effective AML program and address record-keeping and reporting requirements, including requirements to file suspicious activity reports.

One of the core elements of general AML/CFT compliance — established differently for different financial institution types — is the requirement that the provider of the financial service know the identity of the persons to whom it is providing services.

While some financial institutions, such as banks, have prescriptive requirements for customer identification programs,[5] MSBs are also generally required to have in place risk-based policies and procedures for complying with BSA obligations, including verifying customer identification as applicable.[6]

Additionally, financial institutions that are MSBs are required to register with the **Financial Crimes Enforcement Network**.[7]

While implementing these types of measures may create operational complexities given the nature of how some services are delivered, the decentralized finance report makes it clear that the Treasury is not sympathetic to such concerns.

The Treasury simply states in the report that a "DeFi service that functions as a financial institution as defined by the BSA, regardless of whether the service is centralized [or] decentralized, will be required to comply with BSA obligations, including AML/CFT obligations."[8]

This statement — which characterizes a prevailing theme of the new report — appears consistent with the general messaging from the Treasury, and in particular FinCEN, since virtual currency was first introduced roughly 10 years ago.

FinCEN has long interpreted the MSB designation to apply to activities involving accepting, transmitting, exchanging and issuing virtual currencies.

In particular, in a 2013 administrative ruling, FinCEN explained that it viewed the BSA to apply to activities involving virtual currencies in the same manner as they would apply to activities involving "traditional" or "fiat" money, i.e., the "definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies."

FinCEN added that [a]ccepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA."[9]

Since its 2013 guidance, FinCEN has consistently interpreted BSA regulations to apply to virtual currency activities, and has indicated a willingness to interpret the scope of these regulations broadly to encompass new products, services and innovations in the virtual currency space.

For example, in 2019 guidance, FinCEN addressed the applicability of the BSA regulations to certain business models including peer-to-peer virtual currency exchangers, virtual currency wallets, kiosks — or so-called bitcoin ATMs — anonymity-enhanced CVC transactions, and decentralized (or distributed) applications, which FinCEN characterized as "DApps."

With respect to DApps, FinCEN stated that the same regulatory interpretation that applies to other business models — e.g., bitcoin ATMs — applies "to DApps that accept and transmit value," meaning that "when DApps perform money transmission, the definition of money transmitter will apply to the DApp, the owners/operators of the DApp, or both."[10] These statements relating to DApps appear to apply in the context of DeFi more generally.

Application of BSA Requirements to DeFi Services

The report notes that the term "DeFi" has no generally accepted definition but "broadly refers to virtual asset protocols and services that purport to allow for some form of automated [peer-to-peer] transactions, often through the use of self-executing code known as

smart contracts based on blockchain technology."[11]

The risk assessment observes that "DeFi services often provide customers with the same services and products as traditional financial institutions, such as lending, borrowing, purchasing, or trading virtual assets, including assets that function as financial products like securities, commodities, derivatives, or others (e.g., insurance)."[12]

It follows, as indicated in the report, that a "DeFi service that functions as a financial institution as defined by the BSA, regardless of whether the service is centralized [or] decentralized, will be required to comply with BSA obligations, including AML/CFT obligations."[13]

That means that if the service meets the applicable definition of a financial institution like an MSB or a broker-dealer, its decentralization "has no bearing" on whether the obligations apply.[14]

Not only is decentralization seen as generally immaterial to the analysis of whether activity is subject to the BSA, but also the Treasury Department appears to be skeptical of the notion in the first instance.

It cautions in the report that the "degree to which a purported DeFi service is in reality decentralized is a matter of facts and circumstances, and this risk assessment finds that DeFi services often have a controlling organization that provides a measure of centralized administration and governance."[15]

Therefore, after noting money laundering and related risks — e.g., "There have been several instances of actors, including ransomware actors, thieves, scammers, and drug traffickers, using DeFi services to transfer and launder their illicit proceeds"[16] — the report turns to the activities of DeFi services themselves.

The Treasury's view is that "DeFi services at present often do not implement AML/CFT controls or other processes to identify customers, allowing layering of proceeds to take place instantaneously and pseudonymously."[17]

As a result, the report affirms that obligations for financial institutions under the BSA apply to DeFi services, if those services involve the activities of financial institutions as defined by the BSA.

For example, according to the report, if a DeFi service accepts and transmits virtual assets from one person to another person or location by any means, then it most likely would qualify as a money transmitter, and therefore an MSB, and be subject to the same AML/CFT compliance program obligations as a money transmitter offering services in fiat currency.

On the other hand, the report recognizes that some DeFi services may fall outside the BSA definition of a financial institution, such as, depending on the specific facts and circumstances, some services that enable users who self-custody assets to interface with software that processes transactions automatically.

The Treasury Department's rhetoric in describing such services indicates it is also skeptical of decentralization in this context, noting that many DeFi services "claim to be disintermediated by enabling automated [peer-to-peer] transactions without the need for an account or custodial relationship."[18]

Furthermore, the risk assessment notes that DeFi services that fall outside the scope of the BSA could potentially "result in gaps in suspicious activity reporting and limit authorities' collection of and access to information critical to supporting financial investigations."[19]

Other Risk Assessment Findings

The report asserts that bad actors are using DeFi services to transfer and launder their illicit proceeds, largely by capitalizing on vulnerabilities stemming from the lack of AML/CFT controls for DeFi services and lack of compliance with BSA obligations. The Treasury Department identified several vulnerabilities that bad actors capitalize on, including:

- Lack of compliance with AML/CFT obligations;
- Lack of coverage of certain DeFi services by existing AML/CFT requirements;
- Less rigorous or nonexistent AML/CFT controls in foreign jurisdictions; and
- Poor cybersecurity controls by DeFi services.

The risk assessment suggests that such vulnerabilities may stem in part from the fact that industry participants may not fully understand how AML/CFT obligations apply to DeFi services.

While the report may provide further clarity regarding federal agencies' views, the Treasury also relays that the agencies — particularly the **U.S. Securities and Exchange Commission**, **Commodity Futures Trading Commission** and FinCEN — have already made their view known "through public statements, guidance, and enforcement actions."[20]

As characterized by the report, these agencies have already indicated that "the automation of certain functions through smart contracts or computer code does not affect the obligations of financial institutions offering covered services."[21]

Treasury Recommendations, Request for Comment and Implications

The report includes recommendations for U.S. government actions to mitigate the illicit finance risks associated with DeFi services, including:

- Strengthening AML/CFT regulatory supervision;
- Assessing enhancements to the AML/CFT regulatory regime to address gaps;
- Providing additional guidance for the private sector on DeFi services' AML/CFT obligations, as well as coordinating with industry on threat mitigation and information sharing; and
- Engaging with foreign jurisdictions to implement the latest global Financial Action Task Force standards and to close gaps in FATF implementation governing DeFi.

The Treasury Department also seeks public input on the risk assessment — but does not appear to provide in the report a clear mechanism or process to provide such input — and it poses several questions for comment, including which factors should be considered to determine whether DeFi services are a financial institution under the BSA, as well as recommendations for clarifying the DeFi services covered by the BSA and how AML/CFT obligations should vary based on the different types of DeFi services.

Regardless of whether companies in the DeFi space decide to engage with the Treasury and regulators such as the SEC or FinCEN on these issues, it seems clear that federal regulators believe that DeFi services that enable financial products or services such as payments or lending are on notice that applicable activities are subject to regulation under the BSA.

As a result, companies operating in this space will need to consider — or reconsider — how these regulations may apply and how it may be possible to implement controls to meet BSA requirements in spite of delivering services through new technologies.

[1] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance (Apr. 2023), available at: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[2] Executive Order on Ensuring Responsible Development of Digital Assets (Mar. 9, 2023), available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

[3] U.S. Department of the Treasury, National Money Laundering Risk Assessment, available at: https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

[4] Money Laundering Risk Assessment at 1.

[5] 31 C.F.R. § 1020.220(a).

[6] 31 C.F.R. § 1022.210(d)(1)(i)(A).

[7] Id. at § 1022.380.

[8] Decentralized Finance Risk Assessment at 2.

[9] FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013).

[10] Id. at page 18.

[11] Decentralized Finance Risk Assessment at 3.

[12] Decentralized Finance Risk Assessment at 8.

[13] Decentralized Finance Risk Assessment at 2.

[14] Decentralized Finance Risk Assessment at 7.

[15] Decentralized Finance Risk Assessment at 1.

[16] Decentralized Finance Risk Assessment at 16.

[17] Decentralized Finance Risk Assessment at 26.

[18] Decentralized Finance Risk Assessment at 28.

[19] Decentralized Finance Risk Assessment at 29.

[20] Decentralized Finance Risk Assessment at 7.

[21] Id.

Key Contacts

Sean Ruff Washington DC	sruff@cooley.com +1 202 776 2999
Adam Fleisher Washington DC	afleisher@cooley.com +1 202 776 2027
Obrea Poindexter Washington DC	opoindexter@cooley.com +1 202 776 2997