Westlaw Today
powered by Reuters

U.S. Treasury report scrutinizes vulnerabilities in decentralized finance

By John Georgievski, Esq., Lisa M. Lanham, Esq., and Peter D. Hardy, Esq., Ballard Spahr*

APRIL 24, 2023

On April 6, 2023, the U.S. Department of the Treasury released a report[1] examining vulnerabilities in decentralized finance ("DeFi"), including potential gaps in the United States' anti-money laundering ("AML") and countering the financing of terrorism ("CFT") regulatory, supervisory, and enforcement regimes for DeFi.

Ransomware cybercriminals, thieves, scammers, and Democratic People's Republic of Korea cyber actors, have used DeFi services in the process of transferring and laundering illicit proceeds.

The report concludes by making a series of recommendations, including the closing of "gaps" in the application of the Bank Secrecy Act ("BSA") to the extent that certain DeFi services currently fall outside the scope of the BSA's definition of a "financial institution" covered by the BSA. The report cautions that it does not alter any existing legal obligations, issue any new regulatory interpretations, or establish any new supervisory expectations.

AML/CFT risks

The report finds that ransomware cybercriminals, thieves, scammers, and Democratic People's Republic of Korea cyber actors, have used DeFi services in the process of transferring and laundering illicit proceeds. In particular, the report finds that the most significant illicit finance risk exists in the form of DeFi services that are not compliant with existing AML/CFT obligations.

Further, the report finds that "criminals use DeFI services [for transferring illicit proceeds and obfuscating the trail of funds] without being required to provide customer identification information. This can make DeFi services more appealing to criminals than centralized [virtual asset service providers ("VASPs")], which are more likely to implement AML/CFT measures."

Laundering techniques involving DeFi services include the use of decentralized exchanges, or DEXs; cross-chain bridges; mixers;[2] and liquidity pools. After utilizing these laundering techniques, criminals then may use centralized VASPs to exchange virtual assets for fiat currency — often turning to VASPs in jurisdictions with weak or non-existent AML/CFT standards.

The report also observes that most DeFI services conduct transactions using smart contracts that are settled on the public blockchain, rather than through internal order books or ledgers, or a private blockchain. To that extent, such "pseudonymous" transaction information is viewable and traceable on a public ledger.

Public ledgers, in turn, can be used in investigations involving blockchain analytics to trace the movement of illicit proceeds. Nonetheless, the report finds that there can be significant limitations on relying on public blockchain information to trace illicit funds in the DeFi space:

> While regulators, law enforcement, and public blockchain companies can in some cases identify transaction participants, they may in other cases only have the participants' wallet addresses without additional identifying information. Additionally, users can obfuscate the tracing of transactions on the public blockchain through the use of mixers, cross-chain bridges, or anonymity-enhanced cryptocurrencies (AECs), which can create challenges for blockchain tracing. Second, blockchain tracing and analytics often require an initial identified illicit transaction or address as a starting point, although new tools are able to identify potentially suspicious activity based on blockchain data. Third, critical activities in a DeFi service can occur off-chain and there are challenges to locating and obtaining this data.

DeFi defined?

Although the report acknowledges there is no generally accepted definition of DeFi, for purposes of the report, the Treasury defines "DeFi" as "virtual asset protocols and services that purport to allow for some form of automated peer-to-peer ('P2P') transactions."

However, the Treasury stresses that DeFi services often have a controlling organization that provides a measure of centralized administration and governance, including distribution and concentration of governance tokens and voting. Indeed, the report repeatedly expresses skepticism regarding claims of "decentralization," stating that such claims "vary in their

accuracy," can be "overstated," and, "[a]t times, the use of the term [decentralization] reflects marketing more than reality."

The report also critiques industry claims regarding a lack of regulatory clarity, such as what qualifies as a security or whether certain DeFi services meet the definition of a "financial institution" under the BSA. The report comments that the CFTC, FinCEN and the SEC perceive that their public statements, guidance and enforcement actions over the last 10 years "have made clear that the automation of certain functions through smart contracts or computer code does not affect the obligations of financial institutions offering covered services."

The report repeatedly expresses skepticism regarding claims of "decentralization," stating that ... "[a]t times, the use of the term [decentralization] reflects marketing more than reality."

In its report, the Treasury notes that any DeFi service that functions as a financial institution as defined by the BSA will be required to comply with BSA obligations. Specifically, the Treasury notes that if a DeFi service does business wholly or in substantial part in the United States — and 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.

Any such money transmitter would have the same AML/CFT obligations as a money transmitter offering services in fiat currency. Despite this, the report states that some DeFis "purposefully seek to decentralize a virtual asset service in an attempt to avoid triggering AML/CFT obligations, without recognizing that the obligations still apply so long as the provider continues to offer covered services."

That said, the Treasury does acknowledge that certain forms of decentralization activity may not be covered under the BSA. In doing so, the Treasury highlights "disintermediation" activity, which encompasses activity that involves users of unhosted wallets who retain custody of and transfer their virtual assets without the involvement of a regulated financial institution.

However, beyond individual users, DeFis have claimed to be disintermediated by enabling automated P2P transactions without the need for an account or custodial relationship. One issue noted by the report regarding whether activity is truly disintermediated is when an individual or entity retains an administrative key to a smart contract or otherwise is able to change a smart contract, and thereby may have "effective control" over participant assets.

While the Treasury states that these claims need to be evaluated on a case-by-case basis, to the extent such DeFi services are deemed not be covered under the BSA, it would create a vulnerability that could be exploited for illicit activity.

Recommendations

To combat the challenges raised by DeFis, the Treasury proposes several recommended actions:

- **Strengthen U.S. AML/CFT Supervision of Virtual Asset Activities:** This includes outreach to industry to highlight when regulations apply to DeFi services, and based upon feedback, consider taking additional regulatory actions and issuing additional guidance to provide further clarity.
- **Assess Possible Enhancements to the U.S. AML/CFT Regulatory Regime as Applied to DeFi Services:** Enhance the U.S. AML/CFT regime as applied to DeFi services by closing any identified gaps in the BSA to the extent that they allow certain DeFi services to fall outside the scope of the BSA's definition of financial institutions.
- **Continue Research, Private Sector Engagement to Support Understanding of Developments in DeFi Ecosystem:** Monitor any changes in the DeFi ecosystem that could affect illicit finance risks or the application of AML/CFT obligations to entities in the space, via research and engagement with the private sector.
- **Continue to Engage with Foreign Partners:** Working with foreign partners bilaterally to close gaps and implement international standards with regards to virtual assets.
- **Advocate for Cyber Resilience in Virtual Asset Firms, Testing of Code, and Robust Threat Information Sharing:** Advocate for DeFi services to institute real time analytics, monitoring, and rigorous testing of code in order to more quickly identify vulnerabilities and respond to indicators of suspicious activity.
- **Promote Responsible Innovation of Mitigation Measures:** The U.S. government should promote innovation in the virtual asset industry by working with parties who are developing AML/CFT solutions for DeFi services or other tools that could be used by the virtual asset industry to mitigate illicit finance risks associated with DeFis.

The Treasury's report is accompanied by a press release,[3] which notes that this report builds upon Executive Order 14067 ("Ensuring Responsible Development of Digital Assets"),[4] which was previously released in March of 2022.

Notes

[1] https://bit.ly/3H4j8YV

[2] https://bit.ly/41QrKdB

[3] https://bit.ly/43WeXIw

[4] https://bit.ly/3JobhVv

About the authors



John Georgievski (L) is an associate in **Ballard Spahr**'s business and transaction department, focusing on consumer financial services matters. With a background in licensing, he has experience advising clients regarding state requirements for consumer finance products and services, including guiding fintech companies through the regulatory process. He is based in Washington, D.C., and can be reached at georgievskij@ballardspahr.com. **Lisa M. Lanham** (C) is a partner in the firm's consumer financial services group and co-leader of the fintech and payment solutions team. She focuses on financial services matters related to state licenses and federal approvals needed for businesses across the consumer finance industry. Her work includes advising fintech companies on development of products to meet state licensing and regulatory compliance requirements and to obtain and retain approvals necessary to engage in business. She is based in Philadelphia and can be reached at lanhaml@ballardspahr.com. **Peter D. Hardy** (R) is a partner and co-leader of the firm's anti-money laundering team. A former federal prosecutor, he is a national thought leader on the subjects of money laundering, anti-money laundering and criminal tax law. He advises businesses and individuals across industries on government regulatory compliance and enforcement matters involving allegations of misconduct and financial fraud. He is based in Philadelphia and can be reached at hardyp@ballardspahr.com. This article was originally published April 13, 2023, on the firm's website. Republished with permission.

This article was published on Westlaw Today on April 24, 2023.