3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

November 3, 2022

Jon Fishman
Assistant Director, Office of Strategic Policy, Terrorist Financing and Financial Crimes
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

RE: Ensuring Responsible Development of Digital Assets; Request for Comment Document No. 2022–20279

Dear Mr. Fishman:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing to you regarding the U.S. Department of the Treasury's (Treasury) Ensuring Responsible Development of Digital Assets Request for Comment (RFC). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 133 million consumers with personal and small business financial services products. As previously expressed, NAFCU supports the continued development and clarification of a U.S. digital assets regulatory framework that consistently promotes safety and soundness principles, protects consumers and investors, prevents financial crimes, and accommodates responsible technological innovation. NAFCU strongly believes existing anti-money laundering and countering the financing of terrorism (AML/CFT) regulations may be effectively applied to a range of intermediated digital-assets-related finance applications and activities.

However, Treasury and other federal agencies and offices charged with shaping the U.S. digital assets regulatory framework may ultimately determine existing AML/CFT regulations are insufficient to effectively mitigate illicit finance and national security risks arising within some truly decentralized digital-assets-related finance applications and activities. As Treasury executes on its responsibilities outlined in President Biden's March 2022 Executive Order 14067, entitled Ensuring Responsible Development of Digital Assets (Executive Order), Treasury must be sure to not conflate any responsibility to lead the U.S. government's mitigation of digital-asset-related illicit finance and national security risks with a charge to go at it largely alone. NAFCU strongly urges Treasury to work closely with the National Credit Union Administration (NCUA) to ensure it does not deter responsible technological innovation or unnecessarily burden the already well-regulated credit union system as it strives to detect, disrupt, and deter criminals' misuse of digital assets and related technologies.

General Comments

Treasury's annual National Strategy for Combating Terrorist and Other Illicit Financing (National Strategy) features prominently in the Executive Order. Sec. 7(b) of the Executive Order encouraged the Secretary of the Treasury and the heads of other federal agencies and offices to supplement Treasury's 2022 National Strategy with additional views on illicit finance risks posed by digital assets. Sec. 7(c) of the Executive Order required the Secretary of the Treasury, in consultation with the heads of other federal agencies and offices, to subsequently develop a coordinated action plan for mitigating digital-asset-related illicit finance and national security risks addressed in the supplemented National Strategy.

The Action Plan to Address Illicit Financing Risks of Digital Assets (Action Plan) Treasury produced in response to Sec. 7(c) of the Executive Order is thorough in many respects. However, the Action Plan notably fails to discuss digital-asset-related guidance issued by the NCUA. In Letter to Credit Unions No. 21-CU-16, the NCUA recognized federally-insured credit unions' (FICU) authority to establish relationships with third-party providers that, in turn, offer digital asset services to FICU members. The Federal Deposit Insurance Corporation (FDIC) has yet to officially weigh in on identical relationships entered into by its regulated banks. The NCUA subsequently confirmed in Letter to Credit Unions No. 22-CU-07 that FICUs are not prohibited from developing, procuring, or using distributed ledger technologies (DLT) for permissible activities, provided they do so in compliance with all applicable laws and regulations. The FDIC, in FIL-16-2022, entitled Notification of Engaging in Crypto-Related Activities, advised that any FDIC-supervised institution that is currently engaged in *or intends to engage in* any digital-asset-related activities should notify the FDIC. By any measure, the NCUA is actively involved in shaping the U.S. digital asset regulatory framework and encouraging responsible technological innovation within the credit union system.

Though Treasury also excluded credit unions in its October 2021 Report on Stablecoins' primary recommendation that Congress pass legislation requiring stablecoin issuers to be insured depository institutions as the term is defined in the Federal Deposit Insurance Act at 12 U.S.C. § 1813(c)(2), failure to consider the impact of its actions on the credit union system is, unfortunately, hardly unique to Treasury. Sec. 3 of the Executive Order describes the interagency coordination processes contemplated by the Executive order as including Treasury, the Board of Governors of the Federal Reserve System, the Consumer Financial Protection Bureau, the Federal Trade Commission, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the FDIC, the Office of the Comptroller of the Currency, and "other Federal regulatory agencies."

While the Executive Order arguably contemplates the NCUA's inclusion within the broad category of "other Federal regulatory agencies," the Executive Order plainly fails to afford the NCUA the same respect it affords the FDIC. For any component of the U.S. government to exclude, intentionally or otherwise, the Federal prudential banking regulator that is primarily responsible for overseeing nearly 5,000 FICUs that serve over 133 million members and has taken such an active role in shaping Americans' access to digital assets, all but ensures the U.S. digital assets regulatory framework will not be as effective and efficient as it otherwise could be.

Credit Unions' Relationships with Third-Party Digital Asset Service Providers

Millions of Americans already use brokerage, education savings, health savings, and retirement accounts maintained by their credit union's third-party providers to buy, hold, and sell traditional debt and equity securities. A number of FICUs operating under their authority to engage in finder activities, codified at 12 CFR § 721.3(g) and recognized in Letter to Credit Unions No. 21-CU-16, are at the forefront of federally-insured financial institutions establishing relationships with third-party digital asset service providers (digital asset service providers) to offer members and depositors similar access to uninsured digital assets.

As is true with respect to all other activities in which a FICU is engaged, a FICU must ensure its engagement in any finder activity complies with all NCUA regulations and other applicable state and federal laws and regulations. Furthermore, NCUA regulations and safety and soundness principles require that a FICU engaged in a finder activity establish risk measurement, monitoring, and control practices that allow the FICU to ensure the third-party provider complies with and continues to comply with all applicable state and federal laws and regulations, including regulations promulgated by the SEC, CFTC, and Treasury's Financial Crimes Enforcement Network (FinCEN). Subsequent NCUA guidance may recognize FICUs' authority to establish relationships with digital asset service providers that offer FICU members a broader suite of digital-asset-related services. At present, however, all digital-asset-related activities contemplated by the NCUA in Letter to Credit Unions No. 21-CU-16 are intermediated and closely overseen by either a FICU or a digital asset service provider to which existing AML/CFT regulations may be effectively applied.

A FICU may only approve an applicant's membership request once the FICU has, among other things, fulfilled its Know Your Customer (KYC) responsibilities and complied with other applicable AML laws and regulations. Therefore, as a threshold matter, every digital wallet opened by a member through the digital asset service provider with which the member's FICU has established a relationship, and all related transactions, are as attributable to a fully verified member as any other account or transaction in the credit union system. Once a member has opened a digital wallet with a digital asset service provider, a member may fund the purchase of a digital asset with funds held in the member's FICU share or share draft account. Until a member disposes of a digital asset purchased with a digital asset service provider, the digital asset remains in the member's digital wallet hosted by the digital asset service provider outside of the member's FICU. When a member disposes of a digital asset purchased with a digital asset service provider, by selling the digital asset with the digital asset service provider, the member's sale proceeds may either remain in a dollar-denominated form in the member's digital wallet or be transferred back to the member's FICU share or share draft account.

As both the NCUA and Treasury recognize, the SEC and CFTC, or perhaps Congress, must resolve outstanding uncertainties related to the application of securities and commodities laws and regulations to different types of digital assets and related applications and activities. Until these outstanding uncertainties are resolved, the appropriate application of existing AML/CFT regulations to the intermediated digital-assets-related applications and buy-hold-sell activities, contemplated by the NCUA in Letter to Credit Unions No. 21-CU-16 will likely remain less than perfectly clear. However, in this narrow context, a lack of regulatory clarity should not be interpreted as indicating that existing AML/CFT regulations are insufficient to effectively mitigate any related illicit finance and national security risks.

The credit union system has a long history of responsible technological innovation and strong culture of compliance. Credit unions carry on successful, safe and sound relationships with a broad spectrum of third-party providers, many of which are subject to regulation by the SEC, CFTC, FinCEN, and a host of other federal and state regulators. Irrespective of which regulator or regulators are ultimately determined to be responsible for supervising intermediated digital-assets-related applications and activities, credit unions and the NCUA have the capacity to ensure credit unions and their third-party providers fully meet their respective AML/CFT regulatory responsibilities.

Mitigating Illicit Finance Risks in Decentralized Finance

Inconsistent and strained uses of the term decentralized finance (DeFi) within the U.S. government make clear that Treasury and other federal regulators must formulate and uniformly adopt a common, consistent digital assets vocabulary if they are to be capable of mitigating digital-asset-related illicit finance and national security risks across the economy. For example, some digital-asset-related finance applications to which some federal regulators apply the term DeFi are not truly decentralized because they have an identifiable intermediary capable of influencing some or all application functionalities and, in turn, user activities. It appears feasible that Treasury and other regulators may ultimately determine existing AML/CFT regulations, updated to reflect a common, consistent digital assets vocabulary and capable of addressing relatively novel governance structures and mechanisms, may be effectively applied to these types of lightly intermediated digital-asset-related finance applications.

Whether existing AML/CFT regulations may be effectively applied to digital-asset-related finance applications specifically designed to enable users to interact and transact with one another without any intermediary's involvement (true DeFi applications), however, is unclear. Treasury and other regulators may find it particularly difficult, or even impossible, to effectively apply existing AML/CFT regulations to true DeFi applications that enable users to make unlimited real-time peer-to-peer (P2P) payments. Though criminal misuses of digital assets and related technologies may comprise only a small percentage of all digital-asset-related transactions, criminals can misuse true DeFi P2P payment applications to further incredibly harmful, traditionally cash-intensive illicit activities, such as drug smuggling, human trafficking, and terrorism financing. Criminals can also misuse true DeFi P2P payment applications to perpetrate financial frauds that, because true DeFi P2P payment applications lack an intermediary capable of providing defrauded users redress, almost certainly cannot be unwound.

Right-sizing Treasury's Private Sector Engagement

Once outstanding uncertainties related to the application of securities and commodities laws and regulations to different types of digital assets and related applications and activities are resolved, NAFCU is confident that Treasury will find existing AML/CFT regulations can be effectively applied to a range of intermediated digital-assets-related finance applications and activities, including those contemplated by the NCUA in Letter to Credit Unions No. 21-CU-16. If this is the case, there is no reason why Treasury's related interactions with and requirements of the credit union system should change. The NCUA already has all the tools necessary to effectively oversee credit unions' relationships with third-party providers, including their respective compliance with all applicable AML/CFT regulations.

If, however, Treasury ultimately determines it is impossible to effectively apply existing AML/CFT regulations to certain digital-asset-related finance applications and activities, Treasury must be sure to right-size its related private sector engagement. Every day, credit unions play a vital role in mitigating illicit finance risks, including those related to our national security. Beyond ensuring they meet their KYC responsibilities when opening member accounts, credit unions develop and maintain compliance programs dedicated to suspicious transaction reporting, ensuring sanctioned persons and countries do not have a foothold in the American financial system, and training staff to identify personal and transactional behaviors that may conceal or obscure illicit financial activities.

Treasury must remain cognizant that while large, for-profit banks may easily absorb the costs of these resource-intensive compliance programs and other regulatory burdens, many credit unions are very small and have correspondingly modest staff and budgets. Even before Treasury published this RFC, 84 percent of respondents to NAFCU's 2022 Federal Reserve Meeting Survey reported that their credit union's BSA/AML regulatory burden increased over the past five years. 86 percent of respondents expect their credit union's BSA/AML regulatory burden to increase over the next five years. More than half of respondents anticipate their credit union will have to increase the number of full-time employees devoted to BSA/AML compliance within the next three years.

If Treasury determines it must engage the credit union system in order to effectively mitigate illicit finance risks arising within certain digital-asset-related finance applications, NAFCU strongly urges Treasury to work closely with the NCUA to ensure such engagement is not unduly burdensome to credit unions. The NCUA not only has a long track record of effectively overseeing the credit union system for AML/CFT risks but has proven itself as a principled leader in federally-insured financial institutions' engagement with digital assets and related technologies.

Conclusion

As Treasury executes on its responsibilities outlined in the Executive Order, NAFCU strongly urges Treasury to work closely with the NCUA to ensure Treasury does not deter responsible technological innovation or unnecessarily burden the already well-regulated credit union system. Should you have any questions or require additional information, please contact me at dbaker@nafcu.org.

Sincerely,

Dale Ross Baker

Dale Ross Baker
Regulatory Affairs Counsel