ELLIPTIC

July 26, 2021

Federal Deposit Insurance Corporation

Comments@fdic.gov

Re: Request for Information and Comment on Digital Assets

To whom it may concern:

We are writing in response to the FDIC's request for comment on insured depository institutions' (IDIs') current and potential activities related to digital assets..

We greatly appreciate the opportunity to respond to this consultation, and welcome the FDIC's continued engagement with the private sector. As a provider of blockchain analytics solutions that VASPs and financial institutions utilize to comply with anti-money laundering and countering the financing of terrorism ("AML/CFT") regulations, Elliptic is committed to reducing the prevelance of illicit activity in digital assets.

Our recommendations and observations are outlined below. Please do not hesitate to contact us should you have any questions regarding our submission.

Sincerely,

Chris DePow
Senior Advisor - Financial Institution Regulation and Compliance
Elliptic

Reviewing the FDIC's request for comment has made clear that these topics are both broad and deep, with the potential for a sprawling and detailed analysis. In order to keep focus on the key topics attendant to our expertise, and in the interest of succinctness, we will seek to address this request in two parts. Part 1 will address Question 4, "To what extent are IDIs' existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with the various digital asset use cases? Do some use cases more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some use cases result in IDIs' developing entirely new or materially different risk and compliance management frameworks?" Part 2 will address Question 5, "What unique or particular risks are challenging to measure, monitor, and control for the various digital asset use cases? What unique controls or processes are or could be implemented to address such risks?"

Part 1

When determining the extent to which IDIs' existing risk and compliance management frameworks are designed to identify, measure, monitor, and control risks associated with the various digital asset use cases, each individual use case must be examined. There are several components and risk factors, unique to each scenario, that merit individual attention, as a "one size fits all" approach does not work.

Liability-based activities, such as deposit servicing as digital asset reserves, are likely the areas in which IDIs' existing risk and compliance management frameworks are most directly applicable and would require the least technical and procedural enhancement. As noted by the Office of the Comptroller of the Currency in Interpretive Letter 1172:

> *National banks are expressly authorized to receive deposits. Receiving deposits is recognized as a core banking activity. As the OCC recently reaffirmed, national banks may provide permissible banking services to any lawful business they choose, including cryptocurrency businesses, so long as they effectively manage the risks and comply with applicable law, including those relating to the BSA and anti-money laundering.*

Given the willingness of the chief federal bank regulator in the United States to so overtly support the involvement of (at least some) IDI's, and considering the fact that the contemplated deposit services relate to fiat money deposits, industry participants and service providers believe that regulatory risk in this space is relatively low. Existing risk and compliance frameworks are designed to mitigate the risk attendant to holding large cash deposits, including those deposits used as reserves for cash-backed and cash-equivalent-backed assets.

The main financial crime risks associated with an IDI holding fiat reserves that back digital assets are (1) the risk posed by legal or natural persons seeking redemption of digital assets for fiat money and (2) the risk posed by holders of the digital asset that is backed by reserves held at the IDI engaging in illicit activity. In the first instance, IDIs can potentially mitigate the risk by conducting appropriate Customer Identification Program (CIP) due diligence on the person in question, subjecting the person to name screening against applicable sanctions, PEP, and negative media related watchlists, and by monitoring the wallets and digital asset transaction activity associated with the person seeking coin redemption. IDIs must, by regulatory requirement under the Bank Secrecy Act and amendments made via the USAPATRIOT Act, have extant and fully integrated programs to conduct fiat transaction monitoring, customer identification, and name screening.

The obvious opportunity for program uplift with regard to the customer due diligence risk associated with coin redeemers relates to surveillance and evaluation of digital asset-related wallets and transactions. In order to ensure that a customer seeking to exchange a digital asset for fiat money is not attempting to launder “dirty” crypto into “clean” fiat, IDIs must implement a blockchain monitoring and analysis program designed to identify nexuses to and historical transactions with bad actors, including but not limited to dark net markets, sanctioned persons, and terrorist organizations. Such monitoring and analytics programs can, through the use of data science and machine learning analysis, identify potentially problematic instances with a high degree of confidence. Using this data to appropriately risk rate customers and potentially decline transactions allows IDIs to significantly mitigate the incremental risk posed by interaction with the digital asset ecosystem.

Custodial activities, such as providing digital asset safekeeping and related services, are largely, though not completely, covered by existing risk and compliance management policies; however, the implementation of such policies through digital asset-specific procedures will vary greatly across different IDIs. What this means in practice, is that while there are likely “on the books” controls that should be applied to all stores of value, fiat and digital alike, there may not be adequate operationalization of these controls with regard to digital assets. Similar to the aforementioned “fiat reserve” use case, the OCC has provided guidance concerning the permissibility of federally chartered banks serving as digital asset custodians. In Interpretive Letter 1170, they have stated that:

> *National banks have long provided safekeeping and custody services for a wide variety of customer assets, including both physical objects and electronic assets. These functions of national banks are well established and extensively recognized as permissible activities for national banks.23 The OCC concludes, for the reasons discussed below, that providing cryptocurrency*

custody services, including holding the unique cryptographic keys associated with cryptocurrency, is a modern form of these traditional bank activities.

Considering the ongoing support of the OCC and the historical role that banks (and therefore many IDIs) have played in serving as custodians of instruments of value, it's reasonable to believe that IDIs are well positioned to provide digital asset safekeeping services. The demand for such services from investment advisors and other financial services professionals is likely to increase over time, and therefore it's imperative that IDIs implement adequate safeguards early on, so that compliance implementation challenges do not cause customer impacts once interest has piqued.

The "custodial" use case described here presents direct money laundering risks springing from digital asset exposure, unlike the "fiat reserve" use case, which creates only indirect digital asset financial crime risk exposure. IDIs consering acting as custodians must address several specific risks, including (1) the risk that a digital asset held by the custodian is has been used in illicit activity, (2) the risk that the wallet that sent the digital asset to the custodian has been associated with illicit activity, and (3) the risk that the digital asset held in custody was exchanged for an fiat currency or digital asset with a nexus to illicit activity.

All of the above risks may be mitigated through a combination of fiat and digital asset monitoring and due diligence systems. The provenance of all digital assets held by a custodian should be thoroughly vetted through the use of a blockchain analytics provider, so that any prior association of that asset to a bad actor may be determined with a high degree of certainty. All wallets that the custodian receives digital assets from, or delivers them to, should likewise be screened to determine if there is a pattern (or even an isolated incident) of problematic activity being associated with that wallet. Should such problematic activity be discovered , the IDI must leverage it's risk tolerance policies to determine whether it may execute the proposed transaction with the wallet. Lastly, the cross-chain exchange history of the digital asset should be assessed, so that any nefarious activity undertaken in one digital asset ecosystem is appropriately accounted for when evaluating a transaction related to another. If the digital assets in question were previously held at a Virtual Asset Service Provider (VASP), the known risks associated with that VASP itself should be evaluated and should inform the overall risk determination made with regard to the customer and any specific transaction.

Asset-based activities, such as investments, collateral, margin lending and liquidity
facilities, represent a significant increase in the risk exposure posed to IDIs considering entering the space, and also create challenges related to the existing compliance and risk management frameworks currently implemented. Unlike liability-based and custodial activities, transactions related to asset-based activities require

the implementation of new operational and compliance procedures. The exact activity contemplated will also determine the relevant compliance framework that may be required to be uplifted or, in some cases, newly implemented. Further, while other potential use cases have well defined guidance from regulatory authorities, here no such established guidance exists, Instead, IDIs must use their knowledge of common industry practice along with regulatory guidance applicable to similar situations in order to determine the best ways in which to apply their risk based approaches.

The financial crime and regulatory risks presented by asset-based crypto activities will vary significantly, depending on which stripe of the industry an IDI may choose to enter. If the IDI only wants to serve as a fiat on/off-ramp into the world of decentralized finance, then the risks faced may be adequately addressed through customer due diligence, conducted on the VASP that it seeks to allow customer interaction with. This should include not only a thorough review of the VASPs AML and KYC policies, but also of applicable licenses or registrations that may be required to legally do business in the jurisdictions in which it operates, and a review of the entity's underlying operations/technical structure. Part of this can be done by leveraging products such as Discovery from Elliptic, which contains due diligence data on more than 200 VASPs . In this way, most of the risk assumed by the IDI is vicarious, stemming from the underlying service provider that it has partnered with. So long as the VASP in question has a satisfactory AML and KYC program, it is likely that most of the risk may be mitigated.

Should the IDI seek to become a direct player in the world of DeFi, they will have to undertake several meaningful initiatives, related not only to the internal technical buildout of the infrastructure required to support DeFi interaction (or there hiring of service providers/sub-custodians top provide such infrastructure), but also to the design and implementation of a crypto-specific compliance program. The nature of this program will depend on the functional regulation in each jurisdiction, but generally will have to consider (1) the permissibility of the IDI to potentially hold cryptocurrency on a proprietary basis, (2) the tailoring of the IDI's AML/KYC/financial crimes policies to address crypto risk, and (3) the operational risk of entering a new sector.

The question of whether IDIs generally, and banks specifically, may hold crypto on a proprietary basis has remained unanswered for several years, as various regulatory bodies have only tangentially addressed the issue. Based on extant guidance in related areas, it is reasonable to believe that rules and regulations will eventually be instituted, allowing for IDIs to hold proprietary crypto with strong reserve requirements and mandatory risk mitigation strategies. When it comes to tailoring the IDI's financial crimes policies to address crypto risk, there is likely to be a more significant hurdle. On-chain monitoring should be conducted with regard to

every DeFi transaction entered into by an IDI, so as to ensure that no sanctioned (or otherwise problematic) entities or individuals are engaged. This requires either a complete compliance infrastructure build, with systemic integration of blockchain and traditional transaction monitoring and KYC systems, or the use of a third party service provider such as Elliptic, to institute and integrate the required program. Building out such a program from scratch would likely require a significant investment of resources up front, while using a service provider would require less initial investment and enhanced expertise in the space, albeit with ongoing reliance on a vendor. Lastly, the operational risk of entering an entirely new service line cannot be understated.

The business must ensure that the underlying technology supporting the pseudo-financial transaction activity is understood, and that any security or related gaps are identified. The overall risk of the DeFi protocol being leveraged should be accounted for, and appropriate counterparty and infrastructure risk management tools should be employed. A tool such as Discovery from Elliptic may help IDIs to better understand the risk profiles of any centralized VASPs through which DeFi protocols may operate, but the IDI must nonetheless ensure that it conducts ongoing reviews of its crypto related counterparties and service providers, as the risk and regulatory landscape is constantly evolving.

Part 2

Three digital asset usage scenarios present particularly challenging risks to measure, monitor, and control.The first such risk is posed by entities or individuals leveraging tools intended to obfuscate the on-chain history of a transaction. These included Bitcoin “mixing” services. Such tools may make it challenging for compliance departments to identify when a virtual asset has a nexus to a problematic entity or individual and may prevent a financial institution from appreciating the totality of risk presented by a customer.

The second troubling scenario arises from the use of Privacy Coins. Privacy Coins, which are specifically designed to hide the originator, recipient, and value details of a digital asset transaction may seriously impede a financial institution's ability to understand the ultimate origin or destination of a digital asset. Unlike Bitcoin, Ether, and most digital assets, which are highly traceable and can be readily monitored for compliance purposes, most privacy coins are impervious to transaction surveillance. Though the institution may have visibility of book transfers and other internal transactions, any “on chain” activity will largely remain obscured.

Finally, interaction with dApps and DeFi may prove challenging for IDIs to monitor and mitigate. The use of decentralized exchanges, for example, may provide compliance challenges related not only to financial crimes, but to regulatory risk, as the many DeFi platforms are unregulated and may allow the exchange of coins or

tokens with potentially problematic characteristics, such as being classified as securities. Questions surrounding regulation of the credit markets, the implications of staking, and the corporate authority implications of governance tokens provide additional regulatory considerations that must be solved for, in order to adequately mitigate risk.

Controls and processes to mitigate this risk take two forms: transaction level controls and customer level controls. Transaction level controls must include the statistical analysis of blockchain data, in order to form assertions that, with a high degree of certainty, reveal instances of bad behavior and the presence of bad actors. This analysis allows for IDIs to take a risk based approach in determining the potential for financial crime related to a particular wallet or transaction. These blockchain-specific monitoring and analysis solutions should be integrated with the fiat transaction monitoring tools already in place at the IDI, to paint a holistic picture of the risk of a particular transaction and, in aggregate, the customer. It's at this point that customer level controls take over, chief among them the integration of the IDI's risk scoring criteria with the statistical analysis of the blockchain. This integration allows for a risk score informed by alerts/dispositions related to digital asset activity and presents a more accurate and ever-evolving understanding of the customer's risk profile. Examples of such proprietary solutions include Elliptic Lens, which enables interested parties to identify risks associated with a particular wallet, by conducting a data analysis of problematic activity historically engaged in by addresses associated with said wallet.

Customer due diligence should also be enhanced for both natural and legal persons. Natural person's deriving wealth from digital assets should have their source of wealth thoroughly vetted to ensure that the activities that were used to obtain the digital assets were above board. Legal persons should be subjected to the same due diligence and, when deemed to be "Virtual Asset Service Providers" should be required to undergo enhanced due diligence, specifically tailored to assess digital asset AML and regulatory compliance programs.

While there are nearly limitless possibilities for branching and interconnected comments related to this issue, we believe that the information provided above addresses the key risks that IDIs may face when engaging with digital assets. We welcome any feedback that the FDIC or other interested parties may have, and thank you for your time and consideration.