GUIDANCE DOCUMENT

This guidance document is advisory in nature but is binding on an agency until amended by such agency. A guidance document does not include internal procedural documents that only affect the internal operations of the agency and does not impose additional requirements or penalties on regulated parties or include confidential information or rules and regulations made in accordance with the Administrative Procedure Act. If you believe that this guidance document imposes additional requirements or penalties on regulated parties, you may request a review of the document.

Digital Asset Depository Nebraska Operational Consideration Guidance

Nebraska Department of Banking and Finance

Version 2.0 – July 2023

Table of Contents

EXECUTIVE SUMMARY

The development of the Nebraska Digital Asset Depository (DD) Examination Manual and associated procedures has led to the identification of operational risks associated with Custody and Fiduciary Services, Information Security, Payment Systems Risk, and AML/Sanctions. These operational risks were matched to recommendations, including corresponding leading industry practices and processes for risk mitigation.

The recommendations within the four main thematic areas focused on the development of internal controls and governance processes to emphasize the segregation of duties, asset due diligence and ongoing monitoring, integration of new third-party service providers (e.g., pricing vendors, blockchain analytics), and reserve management considerations for stablecoins.

Lastly, a review was conducted of regulatory precedent in addressing material issues within the digital asset space to help guide Nebraska Department of Banking and Finance's (NDBF) approach to remediation.

INDUSTRY BEST PRACTICES

While developing the Nebraska Digital Asset Depository Examination Manual and associated procedures, operational risks associated with each of the substantive sections of the manual have been identified in addition to corresponding leading practices for risk mitigation. Accordingly, a set of recommendations that can be used by NDBF and its examiners to understand what "good" looks like in the industry, surfacing leading tools and processes that capture risk-based controls, has been developed.

The digital asset specific considerations for NDBF and its examiners within the four main thematic areas: Custody and Fiduciary Services, Information Security, Payment Systems Risk, and AML/Sanctions.

1. Custody and Fiduciary Services

The digital assets custody and fiduciary services landscape has witnessed several developments recently, particularly within the key management and safekeeping, and third-party risk management areas.

The following general considerations for examiners relate to digital assets specific nuances for custody and fiduciary activities.

- Key Management
  - Physical storage of digital assets in a cold wallet setup through the use of Hardware Security Modules (HSM)
- Internal Controls and Governance
  - Segregation of duties combined with dual controls for both administrative and operational functions to prevent unauthorized or unilateral access and movement of assets.
  - Asset due diligence including analysis on the features of the digital assets, their supporting blockchains, the developers and miners that support the blockchain protocol, and procedures and documentation and whether the digital assets qualify as securities.
    - DFS provides guidance on some green listed (http://www.dfs.ny.gov/virtual_currency_businesses#bitlicense-faqs)
    - Get no action letter from SEC with regards to custody of a specific digital asset
  - Clear chain of responsibilities with sufficient digital asset expertise to mitigate key-person risk.
  - Data governance and controls to ensure data quality and maintain systems integration.
- Consumer Protection
  - Tiered quorum approach, where different transaction sizes or types would require various levels of approval, with additional access management requirements at the customer level (e.g., biometric data, audio messages) to mitigate risk of fraud.
  - Insurance (where applicable)

  - Disclosures to customers regarding the immutability of transactions and liabilities of the DD through SLAs.
- Asset Valuation
  - Multiple pricing vendors with different valuation methodologies.
- Third-Party Risk Management
  - Initial and ongoing due diligence and oversight of service providers.
- Independent Testing
  - Qualified auditors with digital assets expertise.
  - Qualified model risk management experts to support model validation of systems and pricing methodologies.
- Communication with Regulators
  - Maintain open lines of communication with regulators.
  - Engage regulators early in order to socialize any proposed activities (novel projects).
- Regulators
  - Regulators could join industry groups aimed at sharing information on best practices with other regulatory entities.

2. Information Security

The nature of digital assets and the required technological capabilities to maintain digital asset products and services has elevated information security risk, with implications for cybersecurity and Business Continuity and Disaster Recovery ("BCDR") practices.

The following considerations relate to digital asset-specific nuances within the broader information security framework.

- Ongoing Monitoring
  - Effectively leveraging threat intelligence through a combination of tools and services (e.g., dark web scanning) to continuously monitor risks, allowing the DD's IT team to stay up to date on potential threats, and maintain a more proactive approach.
    - Monitoring for flaws, bugs, and vulnerabilities in the source code for the digital assets that the DD issues or holds in custody, including monitoring for security vulnerabilities that would impact the block verification rules of a digital asset, or could result in the misappropriation of digital assets to an unintended party.
    - Running a node within the blockchain network (DDs would then be aware of a new code release and be able to verify its impact).
    - Monitoring the code source or issuer of the code for security notifications and code updates (Ensuring that software development, whether carried out directly or by a third-party, includes appropriate security testing).
  - Patch management to identify digital asset specific software and source code updates and mitigate risk of incompatibility issues between smart contract code and blockchain code.
- Risk Management
  - Intelligence and risk management integration to alleviate pressure on IT teams and create a more comprehensive cybersecurity strategy (integrating people, technology, and operations capabilities to establish complementary controls across multiple layers

and dimensions of the DD), as opposed to maintaining more manual, time-consuming tasks.
    - Implementation of guidance from the CryptoCurrency Security Standard (CCSS) on the key risks relevant to cryptocurrency storage and usage.
    - Ensuring all internet-facing systems, including those managed by third-parties, are hardened and secured, and penetration tested before going live
    - Appropriate background screening of all employees responsible for manually executed core functions
    - Segregation of duties to ensure that the entirety of a private key, seed or backup mnemonic word phrase related to a private key is not known or accessible by a single person, however components of each part of the seed or backup phrase must be known and accessible by more than a single person
- Software Development Lifecycle
    - Adoption of NIST approach for source or software code used for deploying smart contracts
- BCDR
    - Integration of threat intelligence within the incident response process to allow for seamless and rapid translation of threat intelligence into activation of incident management and BCDR processes
    - Clear chain of responsibilities, definition of the order of operations, and outline of next steps for incident response and threat mitigation
    - Automation of threat intelligence implementation to reduce the workload of IT and Security teams, allowing them to focus on higher priority tasks, determine how to respond to the intelligence being gathered, and ultimately reduce human error
- Board and Senior Management
    - Understanding of risks and regulatory landscape associated with digital assets to provide effective oversight and challenge
    - Understanding of the business value of cybersecurity efforts and investments
    - Presence of technical expertise on the Board to facilitate productive conversation about the DD's cybersecurity posture.
- Training
    - Separate training for information technology staff to focus on digital asset nuances and smart contract risk.
- Independent Testing
    - Qualified auditors with digital assets expertise.
    - Auditing of smart contract code for issued stablecoins.
    - Auditing for information system access and permissions.
    - Auditing of key generation, management, and retrieval.

3. Payment Systems Risk

The development of tokenized assets, particularly stablecoins, has led to an increase in the use cases of digital assets. Payment Systems mainly rely on stablecoins, which elevates the risk of reserve management and governance.

The following includes digital asset specific considerations within payment systems.

- Stablecoin reserve management
  - Transparent and periodic disclosure and reconciliation of stablecoin reserves with participating financial institutions.
  - Third-party audit for stablecoin reserves.
- Stablecoin payment network governance
  - Defined roles and responsibilities for the network participants.
  - Development of clear entrance and due diligence criteria.
- Consumer protection
  - Clear disclosure on redemption right.
  - Transparency on asset classification of the stablecoin reserve.
- Communication with Regulators
  - Maintain open lines of communication with regulators.
  - Engage regulators early in order to socialize any proposed activities (novel projects).

4. AML/Sanctions

The pseudonymous nature of digital assets has heightened the risk of financial crimes. The following includes considerations for examiners as it relates to digital asset-specific nuances (in addition to fiat traditional controls) within the AML/CFT five pillars and the OFAC Framework.

It is noted that in January 2021, Congress passed the AML Act of 2020, which required U.S. Department of the Treasury's Financial Crimes Enforcement Network or FinCEN (in consultation with Federal functional regulators) to promulgate AML/CFT regulations. Due to the addition of the CFT, FinCEN is generally now using the term AML/CFT instead of BSA/AML. For consistency with FinCEN and the other Federal banking agencies, the Department will use the term AML/CFT (which includes BSA/AML) instead of BSA/AML when referring to, issuing, or amending regulations to address the requirements of the AML Act of 2020.

- Board and Senior Management
  - Understanding of risks and regulatory landscape associated with digital assets to provide effective oversight and challenge.
- Customer Due Diligence
  - Online identity verification tools (e.g., Jumio, IDology).
  - Originator / Beneficiary information controls (e.g., first party payments, questionnaires).
- Internal Controls
  - Blockchain analytics tools (e.g., Chainalysis, TRM) for transaction monitoring and sanctions purposes.
  - Transaction and behavioral monitoring
  - AML Asset Due Diligence
  - Effective risk reporting to keep pace with scaling.
  - Geolocation tools and IP address blocking
  - SDN lookbacks
  - Data governance and controls to ensure integration between client and transaction data.

- BSA Officer and Staffing
  - Personnel with digital asset experience
  - Sufficient personnel to support customer and transaction volume spikes due to market volatility.
- Training
  - Training on evolving regulatory landscape and novel red flags.
  - Specialized training on tools, technologies, and new digital assets.
  - Learning management system implementation to support rapid scaling.
- Independent Testing
  - Qualified auditors with digital assets expertise.
  - Qualified model risk management experts to support model validation of systems and blockchain tools.
- Risk Assessment
  - Inherent risks due to supported digital assets, novel products/ services, customer types, rapid growth, on-chain transactions, geographic exposure, and online onboarding.
- Regulators
  - Regulators could join industry groups aimed at sharing information on best practices with other regulatory entities.
  - Training on blockchain analytics to better understand relevant processes prior to department undertaking AML examination of DDs.
- Additional Considerations
  - Travel rule compliance and best-efforts approach.
  - Hosted vs. unhosted wallets identification (where feasible).

REMEDIATION PROCEDURES

In order to develop an approach for addressing material issues at DDs, it helps to consider how other regulators have responded to digital asset issues in the past (as in the sections below which use past cases from the OCC, SEC, and CFTC to illustrate). Nonetheless, the framework for resolving such issues mirrors how other types of material non-compliance (i.e., non-digital asset issues) are addressed.

- Generally, if a material issue is detected that has not been remediated and ranks high in time, complexity and/or scope, regulators require that the non-compliant party submit a remediation plan with specific actions and timelines by a predetermined deadline. Once the remediation plan is received, the regulator then responds and either accepts the plan or rejects it and discusses any modifications they would like to see. Once the plan is agreed upon, the regulator and the firm conduct checkpoint meetings to critically assess progress. Finally, the regulator fully verifies remediation and closes out the issue when there are no material outstanding items for the firm to address.
- If a material issue is detected that has a binary solution (e.g., ceasing to offer an unapproved or unregistered digital asset product or service), the regulator provides a deadline by which the issue must be resolved and conditions that must be met in order for the firm to continue operating in a compliant fashion (e.g., mandatory regulatory filings and deadline to register the previously unapproved product or service).
- If a material issue is detected which the firm claims to have already resolved, the regulator requires sufficient evidence and attestations as to their remediation and adequate measures for ongoing compliance. The regulator may also complete remediation validation.

Below is a summary of three cases at key federal regulators illustrating remediation of material issues arising from digital asset products and services offered by entities under the purview of those regulators.[1]

1. OCC: Anchorage Consent Order, 2022

The OCC filed a consent order against Anchorage Digital Bank ("Anchorage"), due to deficiencies in their BSA/AML and Sanctions Compliance program. The consent order highlighted the following corrective actions.

Within 30 days: Submit an action plan detailing the remedial actions necessary to achieve and sustain compliance with the Bank Secrecy Act ("BSA") and to address all BSA/AML deficiencies, violations and corrective actions communicated to Anchorage, including a description of the corrective actions, reasonable and well-supported timelines, and the person(s) responsible for completion of the corrective actions.

Within 90 days: Anchorage's Board shall ensure that Anchorage develops, implements, and thereafter adheres to an acceptable, written suspicious activity monitoring and reporting program to ensure the timely and appropriate review and disposition of suspicious activity alerts and case

[1] Including paraphrased language from the relevant orders.

investigations, and the filing of SARs. Anchorage's Board shall also submit to the Assistant Deputy Comptroller, for a prior written determination of no supervisory objection, the name and qualifications of a proposed independent, third-party consultant to review and provide a written report on Anchorage's suspicious activity monitoring. This is followed by additional corrective procedures.

Within 180 days: Anchorage's Board must oversee a review of the leadership, knowledge, training, and skills of Anchorage's BSA Officer and supporting staff as well as the adequacy of staffing levels.

2. SEC: BlockFi Cease-and-Desist Order, 2022

The SEC filed a cease-and-desist order against BlockFi Lending ("BlockFi"), a leading digital asset lending platform, due to BlockFi violating Section 7(a) of the Investment Company Act by offering and selling securities without a registration statement filed or in effect with the Commission and without qualifying for an exemption. BlockFi had to undertake the following to satisfy the SEC's conditions for remediation.

Immediate: BlockFi had undertaken to cease offering the relevant product to new investors in the United States and cease accepting further investments or funds for that product by current U.S. investors.

Within 60 days: BlockFi had undertaken to come into compliance with Section 7(a) of the Investment Company Act by either filing a notification of registration pursuant to Section 8(a) of the Investment Company Act (and then within 90 days of filing such notification of registration, filing a registration statement with the Commission, on the appropriate form) or completing steps such that BlockFi is no longer required to be registered under Section 7(a) of the Investment Company Act and providing the Commission staff with sufficient credible evidence that it is no longer required to be registered under the Investment Company Act.

3. CFTC: Tether Order, 2021

The CFTC filed an order instituting proceedings against the issuing entities behind the U.S. dollar tether stablecoin token ("USDT") issuer Tether Holdings Limited, Tether Operations Limited, Tether Limited, and Tether International Limited (collectively, "Tether"), due to misrepresentations to customers and the market that Tether maintained sufficient fiat reserves to back every USDT in circulation "one-to-one" with the "equivalent amount of corresponding fiat currency" held in reserves by Tether, and that Tether would undergo routine, professional audits to demonstrate that it maintained "100% reserves at all times." Tether submitted an offer of settlement, which the CFTC accepted. The corrective procedures highlighted Tether's engagement in remediation efforts, including but not limited to the segregation of operational funds from the stablecoin reserves, and implementation of more automated processes for tracking and updating bank balances and reporting information about the stablecoin reserves.