NEBRASKA
Good Life. Great Opportunity.
DEPARTMENT OF BANKING AND FINANCE

Proposed Digital Asset Depository Nebraska Custody and Fiduciary Services Examination Manual

Nebraska Department of Banking and Finance

Version 1.0 – October 2022

Table of Contents

1. INTRODUCTION

The Nebraska Department of Banking and Finance ("the Department") Digital Asset Depository ("DD") Custody and Fiduciary Services Examination Manual (or "DD Custody and Fiduciary Manual" or "Manual"), provides guidance to Department Examiners in connection with their examination and supervision of digital asset custody and fiduciary activities at Digital Asset Depositories ("DDs").

This Manual is focused on the unique risks and considerations presented by digital assets, and should be read in conjunction with the following existing examiner guidance on custody and fiduciary products, such as:

- FFIEC Trust and Asset Management Services[1]
- Federal Reserve Examination Manual[2]
- FDIC Trust Examination Manual[3]
- Custody Services: Comptroller's Handbook[4]
- Comptroller's Handbook: Asset Management Personal Fiduciary Activities[5]
- Comptroller's Handbook: Asset Management[6]

The guidance contained herein is intended to supplement those and other existing supervisory materials and to identify and discuss the specific considerations and novel risks presented by digital assets. None of the guidance contained herein is intended to replace or relax existing standards. Moreover, this Manual does not aim to completely reproduce existing guidance that applies to custody and fiduciary activities more generally.

Each DD is different and may present unique issues. Accordingly, examiners should apply the guidance in this Manual consistent with each DD's individual circumstances and risk profile, supplemented by the examiner's judgment. This manual borrows material from the sources cited above.

1.1. Overview

A custodian typically offers services related to the settlement, safekeeping, and management of securities, cash, and other assets. A custody relationship is contractual, and the specifics of these services may significantly vary between both custodians and customers. Traditional custodians have provided custody services to banks, mutual funds, retirement plans, bank fiduciary and

[1] Federal Financial Institutions Examination Council (FFIEC). "FFIEC BSA/AML Risks Trust and Asset Management Services" (2014).

[2] The Federal Reserve (FED). " Commercial Bank Examination Manual" (2022).
[3] Federal Deposit Insurance Corporation (FDIC). "Trust Examination Manual." (2005).

[4] Office of the Comptroller of the Currency (OCC). "Comptroller's Handbook booklet, 'Custody Services'." (2002).
[5] Office of the Comptroller of the Currency (OCC). "Comptroller's Handbook booklet, 'Personal Fiduciary Activities'." (2015).
[6] Office of the Comptroller of the Currency (OCC). "Comptroller's Handbook booklet, 'Asset Management'." (2000).[i]

agency accounts, bank marketable securities accounts, insurance companies, corporations, endowments and foundations, and retail customers.

A DD with appropriate expertise and capability might offer any of these traditional custody services for digital assets. A DD may also offer specific custodial services designed to meet or complement the unique characteristics of digital assets. For instance, some digital assets offer "staking" opportunities through which the asset holders can earn benefits by participating in certain network processes. A DD may wish to offer services to assist their clients in participating in staking opportunities. This service may include the facilitation of staking opportunities through an approved third-party. This Manual discusses the unique considerations and challenges that arise when extending custody and fiduciary services to digital assets and establishes an examination program for these activities.

Digital assets present unique risks to a custodian. The lack of a central authority and the immutable nature of some types of digital asset transactions mean that a digital asset holder has no redress in the case of theft or inadvertent data corruption, irrespective of cause or circumstances. Moreover, the ledgers that underlie digital asset networks, by design, are public. These characteristics present significant security and information technology considerations. The security and management of digital asset private keys are a crucial component of a digital asset custodial operation. A substantial section of this Manual will focus on supervisory considerations and examination procedures applicable to this topic.

DDs may offer custodial services to other regulated entities such as investment advisers, investment companies, broker-dealers, future commission merchants ("FCM"), commodity pool operators ("CPOs") or swap dealers ("SDs") regulated by the Securities and Exchange Commission ("SEC"), the Commodity Futures Trading Commission ("CFTC") or other regulators. Specific examination considerations related to these client types are included in this Manual. However, with digital assets continuing to evolve it is imperative that DD management will need to adjust as new guidance becomes available, specifically regarding custodial relationships.

DDs may engage in fiduciary activities with or on behalf of their clients. This occurs when a DD exercises discretion over customers' accounts or assets, typically through trust services. The responsibilities of a depository institution are considerably higher when a fiduciary relationship exists, and this examination guidance reflects an enhanced level of diligence dependent upon how, and by whom, discretion is managed and applied.

The unique characteristics of digital assets presents considerations to many other aspects of a DD's operations and risk management program. This will include the cost and availability of insurance coverage, the structuring of custody agreements, the development of audit programs, and the use and management of third-party vendors, among others. This Manual lays out an examination framework that considers these and other topics. Undeniably, however, this is a nascent industry, and examiners must be vigilant and stay attuned to industry developments. The Department will modify and supplement this examination Manual as needed.

1.2. About Custodial and Fiduciary Services

Custody by a DD (bank or investment adviser[6]) means holding client funds or assets, directly or indirectly, or having the authority to obtain possession of them. For example, an investment adviser has custody when the adviser has possession of client funds and/or assets or has power of attorney to sign checks on a client's behalf, to withdraw funds or securities from the client's account, including fees, or to otherwise dispose of a client's assets for any purpose other than authorized trading. A custodial relationship itself alone is not fiduciary. However, a custodian may provide additional DD services in connection with a custodial relationship, such as trust services that include permissible activities as outlined within the Nebraska Financial Innovation Act[7] ("NFIA"), which will form a fiduciary relationship. Given the discretionary nature of a fiduciary relationship, the standard of care is substantially higher for service offerings in this area.

Custodians serve an essential role in financial and digital asset markets. Custodians hold assets on behalf of their clients. Custodians also often directly interface with exchanges to facilitate the trading of assets, as well as with clearing organizations to facilitate the efficient and orderly clearing and settlement of transactions. Custodians, along with clearing organizations, are therefore sometimes informally analogized as the plumbing of financial markets. Another key role of custodians is providing for the safekeeping and servicing of assets. This is particularly important in the digital asset arena where the loss, theft, or corruption of digital asset keys can jeopardize the control and value of digital asset holdings. Given this unique aspect of digital asset custody, there will be a substantial emphasis on related considerations throughout this Manual.

The NFIA specifies that a DD is authorized to provide digital asset and cryptocurrency custody services.[8] Additionally, DDs may issue stablecoins (digital payment tokens reflecting fixed fiat presentment value), carry on a nonlending of fiat money digital asset banking business for customers, and provide payment services upon request of a customer. Finally, though prohibited from fiat currency lending, a DD may facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to, controllable electronic record exchange, staking, controllable electronic record lending, and controllable electronic record borrowing.[9] Refer to *10. Asset Lending* section of the Manual for more information on the facilitation of asset lending transactions on behalf of custody customers.

Addition detail on the nature of custodial and fiduciary relationships is provided in the sections *Fiduciary Considerations* and *Custody Services* below.

[6] See the SEC's discussion of custody at "Investor Bulletin: Custody of Your Investment Assets" (March 2013).
[7] Neb. Stat. §§ 8-3001 to 8-3031 (LB 649, 2021)
[8] Neb. Rev. Stat. § 8-3024(1) (LB 707, 2022)
[9] Neb. Rev. Stat. § 8-3005 (LB707, 2022)

2. RISKS ASSOCIATED WITH CUSTODY AND FIDUCIARY SERVICES

Commensurate with existing processes, the Department assesses DD activities including custody and fiduciary services risk with respect to its impact on capital, earnings, liquidity, and other risk areas separately from bank or affiliated bank operations. The Office of the Comptroller of the Currency, in Interpretive Letter 1179, states that "a bank should specifically address risks associated with cryptocurrency activities, including, but not limited to, operational risk (e.g., the risks related to new, evolving technologies, the risk of hacking, fraud, and theft, and third party risk management), liquidity risk, strategic risk, and compliance risk (including but not limited to compliance with the Bank Secrecy Act, anti-money laundering, sanctions requirements, and consumer protection laws)"[10]. The Department has defined seven categories of risk for DD supervision purposes in addition to traditional CAMELS: credit, market (including interest rate, foreign currency translation and price), liquidity, operational, compliance, strategic, and reputation. These categories are not mutually exclusive; any product or service may expose an DD to multiple risks. For analysis and discussion, however, the Department identifies and assesses the risks separately.

2.1. Operational Risk (including Transaction, Technology, and Theft/Loss Risk)

Operational risk is the current and prospective risk to earnings or capital from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information. Risk is inherent in efforts to gain strategic advantage, and in the failure to keep pace with changes in the financial services marketplace. Operational risk is evident in each product and service offered. Operational risk encompasses product development and delivery, transaction processing, systems development, computing systems, the complexity of products and services, and the internal control environment.

Operational risk is inherently high in custody services because of the high volume of transactions processed daily. Errors in corporate action, settlement, and operating (suspense) account processing are common causes of losses attributable to custody activities. These losses, individually and in the aggregate, may be material. Effective risk identification and control can greatly mitigate these errors.

The unique characteristics of digital asset custody elevate the inherent level of operational risk of custodial services. Digital assets rely on technology platforms that are not under the control of the DD. In many cases, the administration of these platforms (or networks) is governed diffusely by a large collection of actors through cryptological procedures. Possession or control of a digital asset is typically established through use of a private key. Digital assets are designed so they can be quickly transferred, and transactions are typically (initially) immutable. These features pose unique and substantial risks for a digital asset custodian, and DDs should expect to devote resources to develop robust information security controls and risk management processes. Digital asset custody

[10] Office of the Comptroller of the Currency (OCC). "Interpretive Letter 1179"

typically involves holding digital asset keys on behalf of customers, and all the risks arising from the potential theft or loss of these keys must be managed by the custodian.

Effective policies and procedures, a strong control environment, and efficient use of technology are essential risk management tools. Meaningful reporting, based on accurate and reliable data, is needed to provide management with monitoring tools. The risks may be magnified in a global custody operation where transactions occur around the clock in a variety of different markets. A global custodian must consider a variety of additional factors including differing market rules and conventions, the degree of automation in the various markets, different types of securities, capital or currency restrictions, and the availability and communication of timely and accurate information.

2.2. Liquidity Risk

Liquidity risk is the risk to current or projected financial condition and resilience arising from an inability to meet obligations when they come due. Liquidity risk includes the inability to access funding sources or manage fluctuations in funding levels. Liquidity risk also results from the failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value.

The nature of liquidity risk has evolved in recent years. Increased investment alternatives for retail depositors and off-balance-sheet products with complicated cash-flow implications are examples of factors that complicate liquidity risk.

Digital asset custody and fiduciary services pose particularly heightened liquidity risks due to the unique characteristics and operational complexities of digital assets. Digital asset products or services may affect current or future funding costs, introduce, or increase the volatility of asset/liability mismatches to be hedged or managed, increase the rate of credit-sensitive liabilities, or affect the ability to meet collateral obligations.[11]

DDs that issue stablecoins are subject to NRS § 8-3009 of the NFIA that requires them to maintain unencumbered liquid assets denominated in United States dollars valued at not less than one hundred percent of the value of any outstanding stablecoin issued by the DD[12]. Additional details are provided in the *Nebraska Payment System Manual.*

2.3. Market Risk

Market risk is the risk to current or projected financial condition and resilience arising from movements in interest rates and changes in the value of either trading portfolios or other obligations that are entered into as part of distributing risk. The broader category of market risk includes interest rate risk and price risk.

Interest rate risk is the risk to current or projected financial condition and resilience arising from movements in interest rates. Interest rate risk results from differences between the quality and timing of cash flows. The rate changes and the timing of cash flows (repricing risk); from changing

[11] Office of the Comptroller of the Currency Bulletin 2017-43
[12] Neb. Rev. Stat. § 8-3009(1) (LB707, 2022)

rate relationships among different risks (often reflected in changing quality-based yield curves) affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in financial products (options risk).

The assessment of interest rate risk should consider risk from both an accounting perspective (i.e., the effect on accrual earnings) and an economic perspective (i.e., the effect on the market value of portfolio equity). In some organizations, interest rate risk is included in the broader category of market risk. In contrast with price risk, which focuses on portfolios accounted for primarily on a mark-to-market basis (e.g., trading accounts), interest rate risk focuses on the value implications for accrual portfolios (e.g., held-to-maturity and available-for-sale accounts).

Specific to custodied assets, DDs should ensure that investments are managed prudently, consistent with safe and sound practices, in a manner that (i) addresses interest rate risk, including gap, basis and options risk, (ii) prevents mismatching, and (iii) accounts for potential stress scenarios.

Price risk is the risk to current or projected financial condition and resilience arising from changes in the value of either trading portfolios or other obligations that are entered into as part of distributing risk. These portfolios typically are subject to daily price movements and are accounted for primarily on a mark-to-market basis. This risk occurs most significantly from market-making, dealing, and position-taking in interest rate, equity, commodities, and credit markets. Price risk also arises from DD activities whose value changes (earned and unearned) are reflected in the income statement, such as facilitation of digital asset lending, borrowing, and staking through third parties.

Digital asset custody and fiduciary services pose heightened price risk given historical price volatility and quickly changing prices of virtual currencies or other digital assets, which could present material risks to the DD's overall earnings. Large increases or decreases in the price of digital assets influence the custody fees that a DD charges, and DDs offering digital asset custody and fiduciary services should monitor for the concentration risk of specific digital asset types in addition to fiat-based assets held.

2.4. Compliance Risk

Compliance risk is the current and prospective risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain products or client activities may be ambiguous or untested. Compliance risk exposes DDs to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can also lead to a diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and an inability to enforce contracts.

Custody services are contractual in nature, and a DD must ensure compliance with the provisions of all applicable agreements. A strong compliance program should include monitoring the variety of laws and regulations that may affect a custodian's business and reporting any material changes to the customer. Global custodians in particular must be aware of the regulatory environments in

which they operate. Compliance risk may be heightened in foreign markets because different markets have different rules and regulations. These differences make supervision challenging.

Digital asset custody and fiduciary services pose particularly heightened compliance risks due to the nascent, ambiguous, and evolving state of regulation of digital assets. Compliance risks are further heightened due to changes in the structure of digital assets themselves and framework technologies. A DD offering digital asset custody and fiduciary services should commit risk-focused resources to monitoring regulatory and legal changes impacting the institution's supported products, clients, partners, and operations. Furthermore, it is important for directors to ensure that executive management: is cognizant of applicable laws and regulations; develops a system to effectively monitor compliance risk, which will likely include provisions for training and retraining personnel in these matters; and implements corrective action as quickly as possible when violations occur.

2.5. Credit Risk

Credit risk is the current and prospective risk to earnings or capital arising from an obligor's failure to meet the terms of any contract or otherwise to perform as agreed. Credit risk is found in all activities that depend on counterparty, issuer, or borrower performance. It arises any time funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet. The U.S. securities market settlement practice of delivery versus payment ("DVP") substantially reduces counterparty credit risk in the settlement process.

Global custodians may be exposed to credit risk from several sources. First, if a sub-custodian fails, the custodian may have difficulty obtaining its customers' assets. Second, not all markets settle transactions DVP, so there is risk if the custodian delivers assets without receiving payment or pays without receiving securities. Third, in some markets a custodian may offer contractual settlement. In this case, a custodian makes the entries to its customer's account on the contractual settlement date even if the custodian hasn't actually received the cash or securities needed to settle the trade. Here, the credit risk is with the global custodian's customer. Contract provisions should provide for reversal of the transaction if the trade fails, or a specified amount of time passes. For example, if a customer requests the execution of a transaction and the trade fails due to the transaction's inability to be validated and recorded on-chain, contract provisions should require that the transaction be reversed to recredit the customer account accordingly.

Consistent with traditional banking operations, DDs are required to minimize credit risk to the greatest extent possible. DDs may assume, and appropriately monitor and reserve for incidental or de minimis credit risk through the settlement process or other added-value services. Subject to customer agreement and other limitations, DDs may also facilitate direct lending relationships between customers and other market participants through a third party. Such facilitations are discussed in *10. Asset Lending* section below.

2.6. Strategic Risk

Strategic risk is the current and prospective risk to earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.

This risk depends on the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed toward these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

A DD's decision to offer custody and aligned added-value services, particularly in digital asset markets, is a source of strategic risk. The regulated digital asset custody industry continues to evolve, yet competitive and will substantially rely on management and technology for security, efficiency, and marketplace differentiation. A DD will need to commit risk-focused technology resources to remain competitive with other market participants.

2.7. Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the DD's ability to establish new relationships or services or to continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, access to funds, banking service access, increased regulatory scrutiny, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with its customers and community.

While less measurable than other risk factors, the importance of reputation to the long-term success and safety of depository and fiduciary institutions cannot be overstated. The ability of a DD to deliver services as promised is critical to maintaining its reputation. The transaction-oriented custody services business makes a DD's failure to perform a contracted service highly visible to its customer, and the information security sensitivities and immutable nature of transactions inherent in digital asset transactions will only heighten the impact of reputational risks, whether real or perceived.

In addition to the direct reputation risks stemming from the operation of a custody business, a DD's custody customers may also be exposed to other financial and related risks through the assets they hold in their custody accounts. Although losses connected to these risks will not ordinarily directly impact the DD's earnings or capital, some customers may hold the DD at fault. The possibility that these customers will make their claims or allegations public presents further reputation risk to a DD.

Similarly, fiduciary activities are characterized by the application of discretion. The reputation of a DD will be critical in establishing and maintaining the trust that underpins a fiduciary relationship.

The DD also has inherent reputation risk from utilizing third parties to facilitate transactions, including but not limited to, digital asset trading, digital asset lending and digital asset borrowing. Any negative information or news surrounding the third-party the DD has selected to do business with could affect the DD's reputation as well. To mitigate this risk, the DD should conduct thorough and adequate due diligence on any critical third-party entity it will conduct business with.

2.8. Examination Procedures

Objective: To develop an overall conclusion on the quantity of risk assumed by a DD, the examiner should evaluate the quantity of operational, liquidity, market, compliance, credit, strategic and reputation risk assumed by the DD. Only after quantifying these risks should the examiner come to an overall conclusion on the quantity of risk.

Procedure	Comments
Operational Risk (including Transaction, Technology, and Theft/Loss Risk) Operational risk is encountered in custody activities because of the varieties of risks associated with various digital assets, the DD ledgers required to correlate compliance and customer/depositor relationship, as well as the high volume of transaction processing inherent in the business. A DD controls operational risk by implementing a strong administrative and technical environment. Objective: To evaluate the quantity of transaction risk present in the DD's delivery and administration of custody services.	
1. Evaluate the products and services the DD offers. Consider: • New products; • New markets; and • Changes in technology, including forks, source code changes (whether or not supported by the DD) and new settlement mechanisms.	
2. Evaluate the total volume and trend (both dollars and numbers) of transactions processed and the volume and age of exceptions. Consider: • Volume of transactions settled daily; • Percentage of transactions requiring manual intervention; • Percentage of transactions that fail (rejects, trade fails, etc.); • Types of accounts (custody, fiduciary, omnibus etc.); • Delivery/settlement basis; • Types of digital assets; • Counterparties; • Differing consensus mechanisms, including settlement finality; • Volume and age of reconciling items; • Cash; • Securities by depository; and • House accounts (suspense, receivables,	

taxes, etc.).	
3. Review the total market value of all on book assets and a sample of assets held in custody.	

held in custody services accounts. Consider both the size and number of accounts. Consider the impact of volatility on the value of digital asset custody accounts.	
4. Evaluate the significance of system and technology risks identified in IT audits and reviews, and other reviews of the custody services area.	
5. Determine if the DD has designated an employee or committee to be a point of contact for the public to responsibly disclose critical vulnerabilities or other potential exploits and security risks by protocol developers.	
6. Determine if the DD provided to customers the DD's contact information for customers to provide feedback or submit complaints.	
Liquidity Risk DDs offering custody services, depending upon the clearing nature of the asset, may incur varying levels of liquidity risk. Dependent upon the agreement between the DD and customer, the customer's risk appetite for pledging value in the place of asset delivery may demand liquidity in a number of market movements. Such credit extensions must be managed on the DD books with appropriate limitations. Market swing involving extension of credit to a customer, offset as liquidity demand for the institution, includes but is not limited to: asset/liability mismatches that are inappropriately hedged or managed, increase in the rate of credit-sensitive liabilities, or operational restrictions on asset availability. Objective: To evaluate the quantity of liquidity risk related to the DD's custody services activities.	
1. Evaluate the liquidity reserves the DD maintains for each stablecoin that the DD offers. How are liquidity reserves tracked? Based on the DD's activity, are there assets that have less liquidity under certain scenarios?	
2. Evaluate whether the DD maintains unencumbered liquid assets denominated in United States dollars valued at not less than one hundred percent of the value of any outstanding stablecoin issued by the DD[13].	
3. Examine the DD's risk assessment based on price volatility for assets in custody.	

4. Determine whether the DD has any agreements in place that allow for early termination/return of terms and conditions or other areas where the DD faces liquidity events. Review whether the DD accounts	

[13] Neb. Rev. Stat. § 8-3009(1) (LB707, 2022

for such instances (e.g., where the DD may face contractual mismatches and would be required to assume contracts and refund customers.)	
5. Assess the appropriateness of the DD's planning for liquidity events, including as it relates to customers with large balances or periods of high digital asset volatility or trading activity, and whether it runs scenarios on stablecoins.	

Market Risk

DDs offering custody services incur market risk through duration mismatch of DD investments in addition to price volatility of virtual currencies or other digital assets, which could present material risks to the DD's overall earnings. IRR can arise from a variety of sources and financial transactions and has many components including repricing risk, basis risk, yield curve risk, option risk, and price risk.

Objective: To evaluate the quantity of market risk related to the DD's custody services activities.

1. Assess the measures the DD has in place for the management of repricing, yield curve, and volatility risk (on a short-term or long-term basis). Evaluate the risk monitoring and reporting procedures.	
2. Evaluate the fiat-based exposure the DD has based on the composition of its different reserves and the adequacy of the DD's planning for different adverse conditions.	
3. Evaluate the DD's hedging activity for interest rate risk.	
4. Evaluate the DD's planning for interest rate events and stress scenarios development.	
5. Assess the concentration risk of the DD to specific digital asset types and the potential impact on earnings in the event there is a large increase or decrease in price for digital assets where the DD has exposure (e.g., via custody fees).	

Compliance Risk

DDs offering custody services incur compliance risk through contractual relationships with customers as well as through the numerous applicable laws and regulations, both domestic and foreign.

Objective: To evaluate the quantity of compliance risk related to the DD's custody services activities.	
1. Review the nature and extent of custody activities, including new products, services, and markets, including all fiat in and fiat out as well as suspicious activity that may have an impact on compliance risk.	
2. Review the legal risks to the DD associated with the status of digital assets under state, federal and other applicable law, including through regulatory letters or legal opinions or memoranda from in-house/external counsel.	
3. Determine the extent to which the legal relationship between the DD and its customers is substantially clear, especially with respect to the legal status of digital assets, choice of law, disclaimers, waivers, liens, and other unique aspects of an agreement.	
4. Determine the extent to which the legal relationship between the DD and its vendors is substantially clear, based on the factors set forth in #3 above.	
5. Determine the extent to which the DD uses bespoke or standardized customer agreements.	
6. Evaluate the volume and significance of litigation, social media, and customer complaints, including negative news.	
7. Evaluate the volume and significance of noncompliance and nonconformance with policies and procedures, laws, regulations, and prescribed practices.	
8. Determine appropriate sample size to sample accounts to verify compliance with relevant laws and regulations. Consider identified weaknesses in internal control, audit, compliance, or risk management systems when making your decision.	
9. Evaluate any offerings or operations in areas where there have been substantial recent regulatory changes, to ensure compliance with new or altered requirements.	
10. Determine the DD's attitude and approach	

to custody compliance. Assess the extent to which internal processes, controls and procedures contribute to the compliance standing of the DD.	
11. Identify the predominant compliance risks facing the DD over the past year, and those expected to predominate in the coming year.	

Credit Risk

Credit risk is encountered in custody services activities when a counterparty does not fulfill its contractual part of a transaction, and the custodian has to extend or commit its funds to complete the transaction.

Objective: To evaluate the quantity of credit risk incurred in the DD's delivery and administration of custody and fiduciary services.

1. Review any products or offerings where the DD may incur credit risk. Review customer and vendor agreements as necessary and cross- reference with the DD's books and records to determine the financial position of the DD vis-à-vis individual transactions if necessary. Evaluate whether the DD is generally compliant with restrictions on extensions of credit risk.	
2. Review the types and volumes of custody services products that require the DD to use a counterparty. Consider whether relationship is appropriately reflected on the DD books and includes at a minimum: • To the extent applicable, determine that counterparty credit limits including daylight overdraft, pre-settlement, and settlement lines are appropriate. • Determination of credit risk, and administrative controls defined if credit risk is increasing or elevated because of services such as contractual settlement and contractual income payment. • Reach a determination that the DD is appropriately considering the risks if using settlement systems with irrevocable payments, including distributed ledgers, with delivery commitment features, or where settlement is not DVP.	

• The DD has conducted thorough due diligence reviews of its third-party sub-custodians when it provides global custody services.	

• Determine the adequacy of the reserves, and related safeguards associated with any DD offers indemnification against borrower default or other credit risks when the DD offers securities or facilitation of digital asset lending through a third party, and the potential impact of these risks on the financial position of the DD. • To the extent applicable, the DD has been indemnified by other parties for customer transactions.	
Strategic Risk To evaluate strategic risk, an examiner should consider the levels of risk associated with a DD's custody and fiduciary services in relation to the DD's capital, reserves, and strategic objectives. Objective: To evaluate the quantity of strategic risk present in the DD's delivery and administration of custody and fiduciary services.	
1. Review the strategic plan for the DD and discuss with management the strategic objectives the DD has established for its custody and fiduciary activities. Consider the DD's: • Goals for revenue and net income growth. • Current technology capacity assessments. • Future technology needs. • Staffing. • New markets.	
2. Determine whether any weaknesses were identified in other areas that may hamper the DD's ability to achieve its strategic goals.	
3. Are employees effectively trained in the Custody and Fiduciary services offered by the DD?	
4. Is there a formal succession plan regarding key officers that actively work with the Custody and Fiduciary services offered by the DD?	

5. Assess the competitive position of the DD vis-à-vis peer institutions. Discuss risks and opportunities for the DD relating to its competitors.	
Reputation Risk A sound reputation is essential for a bank, whether a community bank, traditional custody bank or a DD. The examiner's estimation of the quantity of reputation risk depends upon the level of credit transaction and compliance risk and the quality of the DD's control systems. Objective: To evaluate the quantity of reputation risk present in the DD's delivery and administration of custody and fiduciary services.	
1. Review the transaction risk, compliance risk, and strategic risk factors to determine whether: • The DD's strategic plan is in place and being followed. • The control structure is appropriate for the volume and nature of the transactions processed. • The compliance and audit programs have adequate policies and procedures for the DD's custody and fiduciary businesses. • The DD's reputation has suffered from lawsuits, complaints, or losses caused by custody or fiduciary service.	
2. Assess the DD's overall reputation in the marketplace. Observe the reception of the markets and the DD's customers to new products or services in the last year and review a sample of news articles, if available, relating to the DD. Also, note trends in customer number and transaction volume in the last year, accounting for the DD's strategic goals, product lines and market conditions.	
3. Assess the extent to which the DD conducted due diligence into third parties through which the DD has facilitated digital asset related business, in addition to the DD's exposure to these third parties.	

Determine the Quantity of Risk

Based on the examination analysis above, the examiner should determine if the aggregate quantity of the DD's risk is low, moderate, or high. A draft Examination Program Template is included in Appendix A, which will guide the examiner through the various steps of this analysis.

3. RISK MANAGEMENT

Examiners should determine whether an DD has adequate systems in place to identify, measure, monitor, and control risks related to custody, fiduciary, and allied value-added services areas, including the ability to do so on an ongoing basis. Such systems include policies, procedures, internal controls, and management information systems governing custody services.

Examiners should assess the quality of the DD's overall risk management and draw a conclusion of whether the risk management is considered strong, satisfactory, or weak. This conclusion should be reached as the final step of the Examination Procedures laid out in sub-section 3.7.

Effective internal controls are essential to an DD's management of the risks presented by custody and fiduciary services. A properly designed and consistently maintained system of internal controls will help management safeguard assets under custody, produce reliable financial reports, and comply with laws and regulations.

3.1. Operational Controls

The importance of operational controls in the custody services area cannot be overemphasized. Custody is a volume-driven, transaction-processing business, and much of the risk associated with it is operational in nature. For this reason, strong operational controls are essential to effectively manage transaction risk.

Separation of Duties

Some risks relating to digital assets, particularly those arising from errors, internal theft, or malfeasance, can be managed appropriately through the division of duties. A DD first segregates administrative and operational functions, and then it segregates duties (both physical and logical access) within the operating system itself. It is the responsibility of management to assess the control environment and ensure that duties and responsibilities are appropriately segregated.

Given the critical role that digital asset private keys play in the ownership and, therefore, the custody of digital assets, Nebraska has adopted specific requirements for the segregation of duties with respect to digital asset key generation and management, which are discussed in *9. Safekeeping of Digital Assets* section below.

Dual Control

Assets under custody must be properly controlled and safeguarded at all times. Dual (or multi-) control procedures are designed to prevent a single individual, acting alone, from transferring or destroying assets, whether traditional or digital. The Department's examiners should evaluate whether DD procedures require dual control in processing of all custody assets, including securities, cash, income payments, and corporate actions, and digital assets.

Accounting Controls

Independent control processes should ensure the accuracy of an DD's records and accounting systems. Accounting controls are used to monitor and measure transactional workflows and their accuracy. Accounting controls include blotters, reconcilement of cash, minting, mining, and asset movements, as well as related clearing and suspense accounts.

3.2. Account Acceptance and Monitoring

The account acceptance process is a first step in risk management of the risks arising from customer relationships. The risks associated with an individual account should be addressed prior to acceptance. A custodian's acceptance process should provide an adequate review of the customer's needs and wants. During the acceptance process, the custodian should also assess whether its duties are within its capabilities, are lawful, and can be performed profitably.

Procedures

A properly documented account acceptance process will provide sufficient information for the DD to make an informed decision. Risk-based procedures should provide DD personnel with "front-end guidance" related to the review and acceptance of new accounts and should include the DD's requirements related to customer due diligence and required documentation.

Assessment of New Business

The due diligence process should ensure that the services the customer wants the custodian to perform are legal (in the relevant jurisdictions) and within the custodian's capabilities. The account acceptance process should include an assessment of the proposed relationship including a review of the products and services needed by the customer, likely transactions (type and volume), and customer information necessary to facilitate custody transactions (such as tax information related to foreign tax relief). The due diligence process should include a review for compliance with anti-money laundering rules. Refer to the Department's *Digital Asset Depository Ant-Money Laundering and Countering the Financing of Terrorism (AML/CFT and Office of Foreign Assets Control (OFAC) Examination Manual* ("*DD AML/CFT and OFAC Examination Manual*") and the *Bank Secrecy Act/Anti-Money Laundering booklet of the Comptroller's Handbook* for more details.

When accepting new business, the DD should consider the operational needs of the account. The DD should consult all applicable departments (including legal, accounting, operations, and compliance) to determine whether it has the capacity to serve the customer without incurring unreasonable costs.

Agreements

Custody relationships are contractual in nature and are essentially directed agencies. The customer is the principal, and the custodian is the agent. The custody agreement is important as a risk management tool. The agreement should clearly establish the custodian's duties and responsibilities. Custody agreements should be standardized when possible, and any deviations

from the standardized agreement should be reviewed prior to acceptance. DDs should consult

with their attorney in the development of the agreement terms, which will need to be periodically reviewed for changes as developments in the legal and regulatory environments for digital assets may require.

Generally, agreements should also:

- Clearly state the legal nature and quality of the asset, including citations to applicable laws as appropriate;
- Clearly establish the account relationship between the DD and its customer, including whether the relationship is contractual (typical for custody), fiduciary (triggered by the exercise of discretion) or other;
- Clearly define the legal structure of the account, including whether the DD and its customers have agreed to a bailment, Uniform Commercial Code Article 8 relationship or other relationship and whether the assets will be held in an omnibus account, individually segregated account, or other structure;
- Clearly layout the range of permissible services for the associated account(s), especially with regards to permissible transactions, such as digital asset lending;
- Discuss how source code changes and ancillary and subsidiary value relating to digital assets will be treated;
- Clearly contain required disclosures under Neb. Stat. § 8-3008, and other applicable federal and state laws;
- Discuss issues relating to customer access to assets and any restrictions on customer access, trading, or withdrawals; and
- Address choice of law, disclaimers, waivers, and liens.

3.3. Management Information Systems

A management information system ("MIS") is a system or process that provides the information necessary to manage an organization effectively. MIS and the information it generates are generally considered essential to internal control. A primary objective of custody services MIS is the management of transaction and operational risks. Sound MIS produces information that is accurate, timely, consistent, complete, and relevant. It allows a DD to measure operational performance to designated benchmarks. While a DD's MIS enables it to determine whether its operations are profitable, it should also provide visibility to management about other essential matters, such as whether internal controls are working. Additional information on internal control environment can be found in the *"Management Information System" booklet of the OCC's Comptroller's Handbook.*

Contingency Plan

A contingency plan is an extension of a DD's system of internal control and physical security. The plans should include provisions for continuance of operation, and recovery when threats may damage or disrupt the institution's data processing support. For example, a DD that relies on an outside servicer for the bulk of its data processing should take steps to determine whether the contingency plans of the servicer are adequate and whether its own plans complement those of the servicer.

Comprehensive contingency planning policies and procedures for all business lines are a responsibility of the board of directors and senior management of a DD. The board is responsible for reviewing and approving the institution's contingency plans annually and documenting the reviews in its minutes. Additional information on contingency planning around key information infrastructure can be found in the Department's *Digital Asset Depository Information Security Examination Manual ("DD Information Security Examination Manual").*

3.4. Fraud Detection and Mitigation

Under Neb. Rev. Stat.§ 8-3007, a DD must comply with the requirements of the federal Bank Secrecy Act guidance and policies. This should include maintaining a program to detect fraud, both internally and externally (e.g., fraudulent/manipulative trading practices). The program should be tailored to the products, customers, complexity, and overall risk profile of the DD. Ideally, the program should be designed to detect fraud in near real-time and enable timely action to mitigate and prevent potential instances of fraud when detected. The DD should also have policies and procedures for the investigation of potential fraud, as well as a defined protocol for addressing and remedying incidents of fraud.

3.5. Third-Party (Vendor) Management

DDs are increasingly dependent on third parties to support key DD functions. Outsourcing arrangements may include trading, lending tax, legal, audit, and information technology solutions. Given the novel information technology and security risks inherent in providing digital asset custody services, DDs may be particularly exposed to risks arising from the use of third parties.

The Department expects a DD to practice effective risk management regardless of whether the DD performs activities internally or through a third party. A DD's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws and regulations

Specific further guidance on the third-party management of information technology and security providers can be found in the Department's *DD Information Security Examination Manual*. More general information on the third-party risk management can also be found in the *OCC Bulletin 2013-29 "Third-Party Relationships: Risk Management Guidance".*

3.6. Audit

A well-designed and executed audit program is an essential component of a risk management program and internal control framework. An effective audit program is increasingly important as DDs expand into new products, services, and technologies, including those related to digital assets. An effective audit program provides the board of directors and senior management with an independent assessment of the efficiency and effectiveness of an organization's internal control system. When properly structured and implemented, the audit function provides important

information about risk levels and the adequacy and effectiveness of control systems that can help management take appropriate and timely corrective actions.

The determination of a suitable audit program for custody and fiduciary activities is the responsibility of the board of directors. While duties may be assigned to a designated committee. This determination should be based on an assessment of business risk and internal control systems and will be reviewed for adequacy and effectiveness by the Department as part of the examination process.

The FFIEC's "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing" provides additional guidance on the characteristics of an effective internal audit function. The policy statement states that internal audit programs should be targeted using a risk assessment that identifies the institution's significant business activities and their associated risks. The frequency and extent of the internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's profile and activities.[14]

A DD should select an audit provider for digital assets based on a holistic approach, obtaining the Departments approval prior to final engagement. Factors a DD should consider in select an appropriate provider includes:

- Reputation and resources, including technology capabilities;
- Knowledge of digital assets;
- Experience working with complex areas or complex financial institutions;
- Existing digital asset clients.

The DD should consider various technology controls as outlined in the Department's *DD Information Security Examination Manual* and *the FFIEC IT Handbook's "Audit" booklet,* as part of its internal audit process.

[14] OCC Bulletin 2003-12"Interagency Policy Statement on the Internal Audit Function and Its Outsourcing" (March 2013).

3.7. Examination Procedures

Procedure	Comments
Strategic Direction and Organizational Structure Objective: To determine whether the board and senior management have provided management with guidance on strategic direction and the organizational structure of the DD's custody and fiduciary services.	
1. Review minutes, resolutions, bylaws, or other documents to determine whether the board of directors or its designated committee has approved and periodically reviewed: • The strategic plan, strategic direction of the custody and fiduciary businesses, and budgeting process. • The organizational structure of the custody and fiduciary businesses, including delegation of the administration to designated persons or committees.	
2. Evaluate the DD's strategies for custody and fiduciary services and products through discussion with management and a review of technology plans. Consider: • Whether custody services are consistent with the DD's overall mission, strategic goals, and operating plans; • The level of management's knowledge of the industry operating systems; • Whether management evaluates internal controls, security risks, and vulnerabilities. • The DD's internal expertise and technical training; • Management's attention to system security monitoring and testing; and • Management's knowledge of and compliance with applicable laws, regulations, and interpretations as they pertain to custody and fiduciary services.	
Policies Objective: To determine the adequacy of policies on custody services.	
1. Determine whether the DD adopted policies incorporate internal controls, account	

acceptance, monitoring, new product approvals, and audit.	
2. Determine whether the DD has adopted policies and procedures specifically required by applicable law or regulation or guidance, including: • Neb. Stat. §§ 8-3001 to 8-3031 (Nebraska Financial Innovation Act); • Neb. Rev. Stat. §§ 8-101.02 to 8-1,143 (Nebraska Banking Act); • Securities and commodities laws, including 17 C.F.R. § 275.206(4)-2. • This Manual or other applicable guidance; • Other policies as required by applicable law.	
Processes Review the DD's custody services to determine whether the board and senior management have provided an adequate system of controls, procedures, and practices for administering the processes needed to perform its custody services. Objective: To determine the effectiveness of the control processes for custody services. Note: The adequacy and scope of the audit coverage may affect the level of examiner testing and sampling of custodial control activities. Evaluate the audit early in the examination process. Refer to the *Federal Financial Institutions Examination Council (FFIEC) Trust and Asset Management Services*.	
1. Evaluate audit's process review of custody services. Consider: • Whether the audit scope covers significant activities and controls. • The quality of the audit reports. • The independence of the audit function, including authority and reporting lines.	
2. Discuss with senior management its control process to gain an understanding of: • The control culture and structure; • The results of any control self-assessment including administrative reviews of custody accounts; • The controls placed on high-risk custody processes (cash movements, asset movements, digital asset key generation and safekeeping, periods of high volatility in digital asset markets, etc.); • The availability of any independent tests of	

the control structure — audits, SSAE 16 also called the SOC 1 reviews, etc.; • Compliance reviews of processes and internal controls used; and • MIS processes used to control high-risk activities.	
3. Evaluate the DD's control process for monitoring the accuracy of the accounting controls for its custody services activities. Consider: • The promptness with which assets are posted to the system; • The process for managing routine and non-routine manual instructions; • The process for confirming that posted debit and credit totals agree with posting totals (including rejects); • The separation of duties between: o Data input and asset balancing functions, and o Authorization and release of assets or funds; • Periodic trial balances; • Valuation sources; • The timeliness of independent reconcilement functions and exception reporting standards (includes aged items) regarding: o Reconcilement and review of deposit account positions; o Reconcilement of assets held at the DD and other custodians; o Reconcilement and review of suspense (house) accounts; and o Internal control standards for follow-up, resolution, and reporting standards for exceptions; and • Evaluate the DD's control process for house accounts, failed trades, and corporate actions. Consider whether: o House accounts are established only after senior management approves their stated purpose; o House accounts are reconciled and reviewed by independent personnel, and aged items have trigger dates for escalation to senior management;	

○ If applicable, all failed trades are appropriately processed and monitored; ○	
Account Acceptance Process Objective: To determine the adequacy of the account acceptance process. (Review any audit or compliance reports for coverage of account acceptance.)	
1. Evaluate the adequacy of the processes for account acceptance and product development for custody services. Select a sample of new accounts received and determine whether: • The DD assessed the account's custody requirements including all affected departments; • Due diligence reviews include customer identification and expected transaction information; • The DD could lawfully service the account and the legal status and structure of the account is substantially clear; • The DD assessed the account's potential to be profitable; • A committee or senior management received notice of the new account (including house accounts) and approved its acceptance; and • Any accepted account failed to meet one or more of the requirements of established DD policy.	
Management Information Systems Objective: To determine the adequacy of the MIS process. (Review any audit or compliance reports for coverage of MIS.)	
1. Determine the types and frequency of reports to management. Consider: • Transaction exception reports (failed trades, AML alert reports, etc.); • Operational exception reports (out-of-balance errors); and • Volume and efficiency reports.	
2. Evaluate the DD's process for determining the adequacy of its custody information systems. Determine whether: • Critical applications or data are identified;	

• Security controls are defined; and • Vulnerabilities associated with custody services are identified.	
3. Determine the effectiveness of the DD's backup process and contingency planning process. Consider: • Frequency of data backups; • Location where backups are stored; • Disaster recovery plan; • Testing of disaster recovery plan; and • Review of MIS plans of third-party services or outsourced vendor if applicable.	
Fraud Detection Objective: To determine the adequacy and effectiveness of the DD's fraud prevention measures.	
1. Does the DD have an adequate fraud detection program that accounts for both internal and external fraud?	
2. Determine the process, products, tools, and methods an DD uses to detect fraud. Are these abilities adequate? Have the tools been appropriately tested by an internal or external process for data quality and accuracy? Do these abilities address both the subjective (risks identified by the DD) and objective risks (risks identified by the examiner or both law, rules, and guidance) of fraud?	
3. Review any identified or reported fraud incidents, determine whether the incidents were successfully detected, and assess the appropriateness of steps the DD took to address the fraud incident.	
Third-Party (Vendor) Management Objective: To determine the effectiveness of the processes designed to evaluate and manage outsourced functions or third-party (vendor) services used by the DD's custodial operations.	
1. Evaluate the DD's risk assessment process for outsourced or vendor services. Consider whether: • Strategic and business plans are consistent with outsourcing activity; and • Senior management and the board of	

directors are involved in outsourcing decisions and vendor selection.	
2. Evaluate the DD's due diligence process in gathering and analyzing vendor information prior to entering a contract. Ensure the due diligence is properly documented. Determine whether management considers: • Vendor reputation; • Financial condition; • Costs for development, maintenance, and support; • Internal controls and recovery processes; • Establishing standards of service; and • The vendor's insurance coverage.	
3. Determine whether the DD has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified and, for information systems, whether contracts address topics in the "Contracts" section of the FFIEC Information Systems Examination Handbook.	
4. Determine whether the DD has a process for evaluating existing vendor services. Consider whether: • Management designates personnel responsible for vendor management; and • Designated personnel are held accountable for monitoring ongoing activities and services.	
5. Determine if the DD has an adequate process to ensure that software maintained by the vendor is under a software escrow agreement and that the file is regularly confirmed as current.	
6. Determine if the DD has an acceptable process in place to manage vendors who provide critical services to support the safekeeping or processing of digital assets. DDs should have processes in place to ensure that the standards applied by these vendors are consistent with those required and applied by the DD itself.	
Controls Objective: To determine whether management has established and implemented an appropriate control system to address the levels of risk arising from its custody and fiduciary services activities.	

1. Determine whether custody and fiduciary activities receive a suitable audit. Consider: • The independence of the audit function, including authority and reporting lines. • The process for reviewing and approving the audit scope, plan, and frequency. • The risk assessment process. • The adequacy of audit management and staffing, including staffing levels and expertise, specifically in digital assets. • The quality of audit reports and supporting workpapers. • The audit scope and whether all significant activities and controls are covered.	
2. Evaluate management's supervision and control of custody and fiduciary activities through audit reports, compliance reports, and MIS reports. As a part of this evaluation: • Determine whether the compliance systems are effective. • Determine whether internal/external audit coverage of issues related to custody services is appropriate. • Assess management's responsiveness to weaknesses or deficiencies identified by the control systems and in audit reports. • Determine whether the MIS systems are adequate for the nature and volume of business being conducted.	
3. Evaluate whether the DD's audit program adequately assesses the control environment.	
Audit Objective: To determine whether the DD has established and implemented an appropriate audit function to address the levels of risk arising from its custody and fiduciary activities.	
1. Determine whether the DD conducts an annual or continuous audit of custody and fiduciary activities.	
2. Determine whether the scope of audit coverage is commensurate with the level of risk associated with custody and fiduciary activities. Determine if audit activities adequately evaluate the following risk areas:	

i. Accuracy and validity of transactions, including movement of custodied assets, customer instructions, scope of customer authority and any resulting errors; ii. Fee calculations, collections, or waivers, consistent with customer agreements, internal policies & procedures, securities, and commodities laws (including applicable exemptions) and industry best practices; iii. Compliance with governing instruments, internal policies, statutory and regulatory requirements, and securities/commodities laws and regulations, including the Securities and Exchange Commission/Federal Reserve Board Regulation R, Gramm-Leach-Bliley Act broker exception rules and Commodities Futures Trading Commission guidance on "actual delivery" of digital assets; iv. Internal routines and controls. v. Account administration, including documentation of the following: • Deposit account activity; • Custodial agreements; • Customer notices and account statements; • Trading, lending, and related activity executed through a third party; • Valuation methodologies; • Value-added services, including staking, and taxation matters; • Trust agreement and court orders; • Income receipts and distributions; • Principal invasions, including appropriate approvals; • Receipt of assets; • Co-fiduciary, grantor, beneficiary, or third-party approvals; • Annual administrative and investment reviews; vi. Management information systems; and vii. Verification of assets, including independent audit required under Neb. Rev. Stat. § 8-1, 141(4) and the SEC Custody Rule. Provide an assessment of management's corrective actions.	

3. Determine whether audit reporting procedures are adequate. Consider the following: • Formal reports are provided to the board of directors or appropriate committee. • Audit reports include a summary of the effectiveness of internal controls. • Audit findings, including actions taken as a result of the audit, are recorded in the board minutes or appropriate committee minutes.	
4. Audit program deviations are reported and approved.	
5. Determine the reason for any change in internal or external auditors.	
6. Evaluate auditor independence. Consider the following: • Whether the in-house audit function is free from undue influence from senior management. • Whether external audit providers perform other services for the institution that could adversely affect the independence of their audit findings.	
7. Evaluate auditor experience and expertise.	

Determine the Quality of Risk

Based on the examination analysis above, the examiner should determine if the quality of the DD's risk management is strong, satisfactory, or weak. An Examination Program Template is included in Appendix A, which will guide the examiner through the various steps of this analysis

4. BOARD AND MANAGEMENT SUPERVISION

DD directors are expected to perform general supervision over a DD's activities. Directors may assign the administration of custody activities to such officers, directors, employees, or committees as they may designate. However, directors retain the overall responsibility for supervision. There is no prescribed requirement organization for a custody operation, as long as the directors are fully aware of, and able to meet their responsibilities.

4.1. Staffing

Capable management and appropriate staffing are essential to effective risk management. Experienced staff, adequate training, and the ability to manage turnover play a major role in a DD's ability to offer high quality and consistent performance of custody and fiduciary services. A DD must carefully compare its staffing levels with the volume of business and the complexity of the services offered. Given the specialized risks and demands associated with the custody and transaction processing of digital assets, the DDs should ensure that they have appropriate expertise within their staff to manage these risks.

If staffing is not adequate to handle the volume of business, DD may accept directly or indirectly unplanned risks, transactions may be poorly executed, and customer service may be adversely impacted. If staffing is not adequate to manage the unique information security challenges of digital assets, the DD may be at risk of significant adverse events such as theft or loss of assets. In either case, the DD may suffer financial and reputational harm.

DDs are required to maintain their main office and the primary office of their chief executive officer in Nebraska, as specified in the NFIA[15].

4.2. Compliance

The board and management are responsible for ensuring that a DD's custody activities comply with applicable laws and regulations. All applicable laws and regulations relevant to the custody and fiduciary business should be identified and communicated to the appropriate personnel. The DD should have a system in place to monitor for compliance with applicable laws and regulations. The compliance program should be overseen by a chief compliance officer, assisted by a compliance team appropriate to the size and complexity of the DD.

Some of the key compliance areas where DDs should ensure appropriate attention is placed include; local law, recordkeeping and confirmation requirements, shareholder communication, mutual fund custody, retirement plan assets, fiduciary activities, anti-money laundering, SEC and CFTC registration or exemption requirements, and asset lending. These will all be covered in additional detail in subsequent sections of this Manual.

[15] Neb. Rev. Stat §. 8-3005(1)(b) (LB707, 2022)

Varying Regulatory Environments

Custodians, particularly global custodians, may be affected by a variety of laws and regulations. In addition to Nebraska and U.S. federal laws and regulations, the custodian may be subject to the laws of other states or the foreign countries in which it offers services. In foreign countries, the global custodian will typically rely on its sub-custodian to understand and comply with local laws and regulations. Specific areas requiring attention when considering the application of other regulatory regimes to custodial services include:

- *Fiduciary capacity*. A custodian who is not exercising discretionary authority or conducting other activities typically viewed as fiduciary in nature may, nonetheless, be considered to be a fiduciary under law in some jurisdictions.
- *Unclaimed property*. Nebraska enacted unclaimed property laws under the Uniform Disposition of Unclaimed Property Act[16]. These laws define abandoned property and require persons or entities to deliver all abandoned property to the state. Employee Retirement Income Security Act ("ERISA") preempts state unclaimed property laws for retirement plan assets. Globally, unclaimed property laws vary widely. Digital assets are generally seen as "intangible personal property" in many U.S. jurisdictions for the purposes of unclaimed property laws.
- *Taxation*. Countries' tax policies on investment income and capital gains differ. The United States may have tax treaties with other countries that provide tax relief.
- *Money laundering or suspicious activity*. To prevent money laundering and other illegal activities, a wide range of laws and regulations exist that requires banks to identify customers and report suspicious activities. The NFIA imposes similar requirements on DDs.
- *Reporting and recordkeeping*. A custodian may be subject to regulatory reporting and recordkeeping requirements in the countries in which it offers services.

Global custodians may further operate in, and be subject to, multiple regulatory environments. A DD operating in multiple jurisdictions, especially globally, must have an effective process in place to identify regulatory and market changes and ensure continued compliance.

Shareholder Communications

The Shareholder Communications Act and implementing SEC regulations address banks' proxy processing. The objective of these rules is to ensure that beneficial owners of securities are provided proxy material and other corporate communications in a timely manner.

Mutual Funds

The Investment Company Act of 1940 and 17 CFR 240.17f address the custody of investment company (mutual fund) assets. In 2000, the SEC revised rule 17f-5, which addresses custody of fund assets outside the United States and added a rule 17f-7 to address custody of fund assets with foreign securities depositories.

[16]Neb. Rev. Stat. §§ 69-1301 to 69-1329.

Anti-Money Laundering Recordkeeping and Reporting

31 CFR 103 addresses bank recordkeeping and reporting requirements for certain financial transactions. Records are required to be maintained for many transaction types including wire transfers, deposit account activity, and certain extensions of credit. Reporting requirements include suspicious activities, currency transactions, and reports of foreign financial accounts. In addition, Nebraska law[17], makes federal BSA/AML/KYC/sanctions regulations applicable to DDs. Chapter 8 further requires that DDs establish and maintain programs for compliance with the federal Bank Secrecy Act as the act rule existed on January 1, 2022. Therefore, to comply the DD should monitor for BSA compliance, conduct risk assessments, use a digital asset analytics provider, establish performance metrics, and adhere to other applicable standards.

For additional information, refer to the *Department's DD AML/CFT* and *OFAC Examination Manua*l and the *"Bank Secrecy Act/Anti-Money Laundering" booklet of the OCC Comptroller's Handbook.*

[17] Neb. Stat. § 8-3002(5) (LB649) and Neb. Rev. Stat. § 8-3005(5) (LB 707, 2022)

4.3. Examination Procedures

Procedure	Comments
Personnel Objective: Given the size and complexity of the DD, determine whether the DD's management and personnel display acceptable knowledge and technical skills to manage its custody and fiduciary services activities.	
1. Using what you have learned from performing these procedures, evaluate the knowledge, communications, and technical skills of management and staff members.	
2. Evaluate whether the staff size is sufficient to manage the volume of business conducted. Consider: • Overtime records. • Turnover. • Plans for further automation. • Strategic direction.	
Shareholder Communications Rules – 17 C.F.R. §§ 240.14-17 govern the distribution of proxy materials and the disclosure of information about shareholders whose securities are registered in a bank nominee name. Objective: To determine the adequacy of the DDs Shareholder Communication procedures.	
1. Determine the process used by the DD to code accounts for beneficiary ownership (OBO or NOBO) to pass information received from issuers, such as proxies and annual reports, to beneficial owners as appropriate (17 CFR 240.14c-2 and 17 CFR 240.14c-101).	
2. Review DD responses to requests for information from issuers to determine whether the responses were appropriate and timely (17 CFR 240.14b-2(b)).	
U.S. Investment Company Assets – 17 CFR 240.17f Objective: Evaluate the DD's compliance with SEC rules governing the custody of Investment company assets.	
1. If the DD is the custodian of investment company assets, determine whether the processes to comply with SEC revised rule 17f-5 and new rule 17f-7 are adequate.	

Escheatment/Unclaimed Property

Procedure	Comments
Objective: Evaluate the DD's approach to handling escheatment and unclaimed Property.	
1. Determine whether the DD's process for escheatment of unclaimed items is appropriate. Consider: • Whether the DD ages outstanding checks, suspense account entries, or house accounts entries. • Whether the DD filed escheatment reports with the proper jurisdiction.	
Lost and Stolen Securities — 17 CFR 240.17f-1 Objective: Evaluate the DD's approach to addressing lost and stolen securities.	
1. Determine whether the DD has written procedures to report lost and stolen securities with the Securities Information Center (SIC). Consider whether: • The DD is registered as a direct or indirect inquirer with SIC. • The DD has a FINS number.	
Other Applicable Laws Objective: Evaluate the DD's approach to monitoring and complying with applicable laws and regulatory requirements arising from all jurisdictions with oversight of the DD's activities.	
1. Determine through inquiry with senior management whether the DD has a process to determine the laws applicable to their custody and fiduciary service activities, and whether they have established processes to maintain compliance with them. Consider: • State and local laws in the United States; • Federal law. • Country laws governing sub-custodians in the network. • Central securities depositories ("CSD") requirements. • Foreign tax regulations and reclaim practices.	

5. FIDUCIARY CONSIDERATIONS

5.1. Background

The Nebraska Banking Act[18] allows financial institutions to exercise fiduciary powers under separate charter under the Nebraska Trust Company Act similar to those permitted to national banks. Fiduciary activities, i.e., fiduciary powers, cover a large range of arrangements in which a DD is retained to, among other things, act as trustee or otherwise exercise some degree of discretion over customers' assets.

A fiduciary relationship is a key component of fiduciary activities/powers. This legal relationship involves a duty on the part of the fiduciary (the DD) to act for the benefit of the other party to the relationship (the customer) concerning matters within the scope of the relationship, usually on a discretionary basis. The fiduciary relationship is designed to protect the party who grants fiduciary power (grantor) to another party (fiduciary) and those who may ultimately benefit from that transfer of power (the beneficiaries) from the significant risks inherent in the fiduciary relationship. The underlying premise of fiduciary law is to afford grantors legal protections that might otherwise be unavailable, too costly, or impractical to obtain. A fiduciary relationship will, generally speaking, involve a higher degree of responsibility—and present a higher degree of legal risk—compared with a purely custodial or safekeeping relationship.

There is no hard and fast rule for determining when an activity or relationship is fiduciary, and as a result, it is a facts-and-circumstances determination. Fiduciary activities may involve investment adviser, investment management, trust protector/trust adviser type-activities. Custody is generally a non-fiduciary activity for Nebraska banks and national banks [19] but can be conducted on a fiduciary basis if the bank is also exercising discretion over the account for investment management or adviser-type activities.[20]

For national banks, "fiduciary capacity" is defined to include "trustee, executor, administrator, registrar of stocks and bonds, transfer agent, guardian, assignee, receiver, or custodian under a uniform gifts to minors act; investment adviser, if the bank receives a fee for its investment advice; any capacity in which the bank possesses investment discretion on behalf of another; or any other similar capacity that the OCC authorizes pursuant to 12 U.S.C. 92a."[21] 12 U.S.C § 92a permits the OCC to authorize and empower national banks to engage in similar activities as state-chartered institutions that national banks compete with.

These regulations are generally permissive and authorize specific fiduciary activities for banks and federal saving associations (FSAs) unless the activities are restricted or prohibited by applicable law. The applicable law for a national bank is defined in 12 C.F.R. § 9.2(b) and for an FSA is defined in 12 C.F.R. § 150.60 as:

- the terms of the instrument, or legal document, governing a fiduciary relationship.
- the law of a state or other jurisdiction governing a bank's fiduciary relationships,

[18] Neb. Rev. Stat. § 8-1, 141(3)(d) (LB649, 2021)
[19] Office of the Comptroller of the Currency, *Custody Services: Comptroller's Handbook*, 11 (2002).
[20] *Id.*
[21] 12 C.F.R. § 9.2(e).

applicable federal law governing those relationships (for example, federal securities laws or the Employee Retirement Income Security Act of 1974), or any court order pertaining to the relationship.

While 12 C.F.R. § 9 and 12 C.F.R. § 150 reflect common fiduciary principles and their provisions are not specific to a particular state law or a type of fiduciary instrument, certain parts are linked to other fiduciary laws, such as the compensation provisions of 12 C.F.R. § 9.15 and the authorization of certain reasonable fees under 12 C.F.R. § 150.380, as well as provisions related to conflicts of interests in 12 C.F.R. § 9.12.

Since a fiduciary relationship involves both the exercise of discretion and a responsibility to safeguard customers' interests, the characterization of a relationship as fiduciary presents significant legal risks and implications, and there is a large and active body of case law relevant to this area.

Compliance with fiduciary law is neither a guarantee against loss nor an assurance of expected performance by the fiduciary. Courts have recognized that even sound fiduciary administration and investment practices can produce unexpected losses. The legal standard to which a bank trustee is held is referred to as the Prudent Person Rule. This means the trustee's action or inaction is viewed by the court against the standard of what a prudent person, with similar skills, would do in a similar situation.

Nearly every state has adopted some form of the Uniform Prudent Investor Act of 1992, including Nebraska[22]. The expectation under these state laws is that if a trustee's investments were consistent with the overall objectives of the account when made, and the investments were made to diversify the client's portfolio, and they do not conflict with the terms of the governing instrument, losses on the individual investments in the diversified portfolio do not mean the trustee violated his or her fiduciary responsibilities.

Given the higher legal standard involved, and elevated risks associated with offering fiduciary services, management should make a careful decision whether to offer this line of service. DDs that choose to offer fiduciary services should recognize the elevated standard of care required, and the skill base necessary to provide that standard of care. Management should notify the Department of their expanded business plans. Similarly, Department examiners should understand the fiduciary responsibilities of an institution under examination and apply appropriate heightened examination standards, as discussed below. In the absence of an affirmative decision to offer fiduciary services, it is important that DDs and their managers, through the account acceptance process, identify the activities and offerings, especially as they relate to digital assets, that may present the potential for fiduciary level duties, and apply appropriate elevated standards of care.

5.2. Fiduciary Services

Fiduciary service offerings have evolved into a comprehensive and integrated selection of financial products and services that permit banks to compete with other financial service providers, such as brokerage firms, investment companies, investment advisers, and insurance companies.

[22] Neb. Rev. Stat. §30-3883

Traditional fiduciary services include personal trust and estate administration, retirement plan services, investment management services, and corporate trust administration.

Banks also provide other fee or transaction-based fiduciary-related services, such as financial planning; trade execution; investment management; cash management; tax advisory and preparation; and advice on, and execution of, financial risk management products, such as derivatives. Fiduciary services are provided through internal bank divisions, subsidiaries (including separately chartered trust banks), other affiliates, and third-party service arrangements.

The increasing importance of fee income is a key factor in the evolution of fiduciary services. Rapid technological advances and a management focus on generating additional revenue sources have enabled banks to base the prices of their products and services on actual delivery costs and internal risk/return profitability standards. Competitive and innovative fiduciary products and services give banks the opportunity to increase and diversify revenue streams.

The DD is permitted to facilitate certain activities, such as digital asset lending and digital asset trading, through a trusted third party. However, facilitation activities in and of themselves do not necessarily trigger a fiduciary capacity. Whether the activities are in fact fiduciary in nature will depend on the facts and circumstances of the DD's role within the facilitation process. There may be instances in which the DD may be acting in a discretionary or fiduciary capacity.

Trusts

A trust is a fiduciary relationship in which the *trustor* gives another party, the *trustee*, the right to hold assets for the benefit of a third party, the *beneficiary*. Trusts are established to provide legal protection for the trustor's assets and to ensure the trustor's assets are managed and distrusted in a prescribed manner. Trusts may be established for additional purposes, including to obtain management efficiencies or to avoid or reduce taxes, particularly estate and inheritance taxes. Nebraska Trust Companies are regulated under Chapter 8, Article 2 of the Nebraska Statutes. Additionally, trust department authority is granted to state chartered banks pursuant to Nebraska Revised Statute § 8-159.

Custodial Activities

Traditional custodial and safekeeping services, which are covered in Section 7 of this manual, generally do not constitute a fiduciary relationship under Nebraska or federal law. Similarly, in the setting of retirement plans, the Department of Labor ("DOL") has ruled that a bank serving solely as custodian is not a fiduciary.[23] However, a custodian may perform functions that are fiduciary in nature. For example, it is not uncommon for a custodian to provide trust services for customer accounts in which the custodian is acting in a fiduciary capacity.

[23] Advisory Opinion 77-45.

5.3. Retirement Plans[24]

The Employee Retirement Income Security Act of 1974 ("ERISA") sets out minimal requirements for the administration of most retirement plans in the United States. ERISA codifies traditional fiduciary responsibilities into a single nationwide standard. The primary section of the ERISA which deals with fiduciary responsibilities is Section 404. The standards enunciated by Section 404 amount to an itemization of how a fiduciary should act. ERISA considerations may apply when a DD facilitates transactions through a third party on behalf of an ERISA plan, depending on the nature of that facilitation.

Fiduciary Defined

For the most part, the definition of a fiduciary under ERISA is a functional definition (see Section 3(21)(A) of ERISA). Therefore, a person is a fiduciary to the extent he:

- Exercises any discretionary authority or discretionary control respecting management of such plan, or exercises any authority or control respecting management or disposition of its assets;
- Renders investment advice for a fee or other compensation, direct or indirect, with respect to any moneys or other property of such plan, or has any authority or responsibility to do so; or
- Possesses any discretionary authority or discretionary responsibility in the administration of such plan.

Certain entities with respect to a plan are automatically fiduciaries: trustees, named fiduciaries, plan administrators and investment managers. This includes the management of the plan sponsor. Every qualified plan must have at least one named fiduciary person designated as the one responsible for operating the plan. This person may be the trustee, the plan administrator, the employer/plan sponsor, or the investment advisor. Fiduciaries generally do not include accountants, attorneys, insurance agents, insurance companies, consultants, or actuaries unless they exercise control over the plan in some fashion.

Requirements

Exclusive Benefit - ERISA Section 404(a)(1)(A): The overall thrust of ERISA is that the plan must be operated solely for participants and beneficiaries of the plan. Section 404(a)(1)(A) expands on this underlying theme by stating that the plan must be operated for the exclusive purpose of providing benefits and defraying reasonable administration expenses. Any violations of ERISA's self-dealing or conflict of interest provisions (Section 406 prohibited transactions) would also normally involve a violation of Section 404.

Prudent Man Rule - ERISA Section 404(a)(1)(B): This section of ERISA requires that fiduciaries act prudently. Prudence is normally associated with asset management, but this section also applies to all of a fiduciary's duties for a plan. The prudence requirement under ERISA includes an implication that a trust department may be held to a higher standard of prudence than

[24] The material presented here substantially draws from the FDIC Trust Examination Manual's discussion of Retirement Plans, which contains additional material on this topic, as noted below, which may be relevant for examinations of retirement plan administration by DDs.

individual fiduciaries. A fiduciary that holds itself out as having a certain expertise (such as a trust department marketing and charging fees for its services and expertise) is to be held to a higher standard of prudence than merely a prudent individual[25]. Examiners should be aware that a plan's exemptions under Sections 407 and 408 from prohibited transactions under Section 406 of ERISA do not release the fiduciary's duty under Section 404 regarding prudence.

The Labor Department[26] has provided guidance on the actions a fiduciary must take in order to demonstrate it was prudent. The regulation does not explicitly state that the appropriate consideration must be in writing; however, documentation is the only logical way a DD could demonstrate prudent actions at a later date. Examiners should note that a DD is not responsible for reviewing the prudence of investment decisions made by outside investment managers to whom investment responsibility has been properly delegated by the plan administrator or other authorized party.

Diversification of Investments - Section 404(a)(1)(C): Section 404(a)(1)(C) of ERISA requires that plan investments be diversified in order to minimize the risk of large losses. Prior DOL rulings indicate an appropriate benchmark of one-third (33%) of the total assets of a portfolio of assets should be used in evaluating whether an investment is diversified. The banking statutory standard of 25% of capital to determine concentrations of credit does not apply to ERISA accounts. While ERISA requires that plan assets be diversified, and failure to do so is a violation, there are a number of specific instances where the diversification standard does not apply that are outlined in the ERISA laws.

Adherence to Plan Document - ERISA Section 404(a)(1)(D): Section 402(a)(1) of ERISA requires that every employee benefit plan shall be governed by a written plan instrument. Failure to follow this governing plan document is normally a violation of ERISA Section 404(a)(1)(D). If the trustee's actions comply with the plan or trust agreement but would violate ERISA, the plan or agreement may not be followed. In such instances, ERISA takes precedence over the governing documents.

Indicia of Ownership of Plan Assets - ERISA Section 404(b): In order to facilitate oversight and enforcement by appropriate agencies, ERISA Section 404(b) requires that documents evidencing ownership of plan assets must be maintained within the jurisdiction of United States (U.S.) courts. These documents (securities, certificates, etc.) are termed indicia of ownership. A number of specific exceptions to holding plan assets which are foreign securities outside the U.S. are outlined primarily in DOL ERISA Regulation 2550.404b-1 and, under certain circumstances, the accompanying Preamble.

NOTE: In addition to the fiduciary obligations directly addressed within ERISA, which have been described above, there is also a host of additional fiduciary considerations that have been identified by the FDIC as warranting consideration during an examination. Given the detailed coverage of these topics there, refer to *Chapter 5 of the FDIC Trust Examination Manual*.

[25] See related discussions of the Prudent Man Rule in the FDIC Trust Examination Manual, Appendix C - Fiduciary Law.
[26] DOL ERISA Regulation 2550.404a-1(b)

5.4. Examination Procedures

Procedure	Comments
Trust and Fiduciary Activities Objective: Assess the overall risk profile and compliance program of the DD's Trust and Fiduciary activities.	
1. Review the fiduciary/trust activities of the DD to determine the DD's risk profile. Consider the following: • Consolidated Reports of Condition and Income Schedule RC-T. • Business plan and charter application. • Other regulatory reports, examinations, investigations, and correspondence from the Department, SEC, Financial Industry Regulatory Authority ("FINRA"), CFTC or Department of Labor. • Public information such as stockholders' reports, the DD's Internet site, press releases, and published news stories. • Current trust department Statement of Assets and Liabilities or trust department Statement of Condition. • From trial balance or other sources (RC-T), profile types of accounts administered (e.g., personal trust, corporate trust, employee benefit (defined contributions, defined benefit), investment management etc.), associated assets under administration, and discretionary management as well as nature of services rendered. • Responses to the First Day Letter and the Officer's Questionnaire. • Customer complaints. • Social media consideration • Pending or threatened litigation.	
2. Determine if fiduciary/trust operations administers or uses common trust funds, investment companies/funds, collective investment funds, proprietary mutual funds, or other pooled investment vehicles.	

Procedure	Comments
Determine the extent to which the DD services these entities as customers.	
3. Review the following information regarding management and supervision of the fiduciary/trust operations: A) Minutes of meetings of the board of directors, trust related committees and subcommittees. B) Organizational charts. C) Committee composition and structure. D) Management information reports, such as: • Net overdrafts and other account liabilities. • Large cash balance reports. • Delinquent fee reports.	
4. Perform a targeted account review. In determining the scope of account review, consider the following: i. General account selection criteria: • Pending or threatened litigation. • Large asset balances or high volumes of transactions. • Customer complaints. • A variety of digital assets, including assets which have shown higher trading interest or volatility. • Previous examination criticisms. • New and closed accounts. • Successor appointments. • Co-fiduciary relationships. • A variety of types of customers (e.g., broker-dealer v. investment company, individual v. institutional) • Accounts for which the DD both provides custody and discretionary services. • Accounts where the DD has explicitly disclaimed status as a fiduciary. • Internal watch lists and, to the extent applicable, accounts risk rated inherently "high" (e.g., ERISA-governed accounts).	

Procedure	Comments
• Assets not carried on the department's books. • Accounts with liabilities. • Accounts lacking diversification. • Administratively complex assets held in discretionary and investment advisory accounts. ii. Actual or potential conflicts of interest, such as: • Discretionary investments in own institution or parent securities and deposits. • Discretionary investments in securities and other obligations of insiders. • Discretionary investments in proprietary products (mutual funds, insurance, and annuities). • Inter-trust transactions. • Accounts where insiders serve as co-fiduciary. iii. Employee benefit accounts with plans that: • Cover the institution's employees. • Are sponsored by directors or their related interests. • Are under investigation by the Department of Labor. iv. Corporate accounts with issues that are: • In default. • Subject to the Trust Indenture Act of 1939. v. Estates that have been open for an extended time.	
5. Assess the effectiveness of the DD's internal control practices in protecting and controlling fiduciary/trust assets. Controls include the following: i. Fiduciary/trust assets should be separated from the assets owned by the institution and may be required to be further segregated based on federal law, Nebraska law or customer agreement, as applicable.	

Procedure	Comments
ii. Appropriate recordkeeping in line with fiduciary/trust best practices. iii. All other legal requirements have been met (appropriate fiduciary/trust agreement, etc.). iv. Controls over the receipt and release of assets should include the following: • More than one institution employee must be present when assets are received. • Account holders or beneficiaries should sign written confirmations for all items distributed to them. v. Assets held by the DD, and by third parties acting on behalf of the DD, are subject to procedures and standards for safekeeping outlined in Chapters 8 and 9 of this Manual. vi. Control procedures for worthless assets should include the following: • The value of worthless assets should be appropriately researched, documented, and periodically reviewed. • Worthless assets should be maintained on the department's books at nominal value. vii. Hold and return mail procedures provide proper controls. viii. Ensure adequate procedures and processes are in place to handle bounce back or incorrect email addresses for customer accounts ix. Controls over the disbursement of fiduciary/trust funds should address the following: • Controls over unissued checks, including the use of sequential or prenumbered documents. • Signature controls. • Wire/ACH controls. • Digital asset-specific controls consistent with standards and procedures outlined in Chapters 8 and 9 of this Manual.	

Procedure	Comments
Conflicts of Interest Objective: Assess the DD's policies for the management of conflicts of interest.	
1. Determine if the DD identifies and monitors actual and potential conflicts of interest and self-dealing. Consider the following potential conflicts: • The use of material inside information, including information arising from commercial bank relationships or customer market positions to benefit the DD or other customers. • Use of own-DD products and services, including deposit accounts, payment instruments, stablecoins issued by the DD, and ancillary services involving stablecoins issued by the DD. • Receipt of fees from other sources, including but not limited to custody, trading fees, exchange fees, and sweep fees. • Relationships with brokers, dealers, digital asset exchanges, investment advisers, commodities intermediaries, digital asset networks, payment networks, banks, and other agents, including soft dollar arrangements. • Investment in own-DD or affiliated securities and other transactions involving insiders or their interests. • Proxy voting, including own-DD or affiliated securities. • Investment in securities underwritten by the DD or affiliates. • Inter-account and multi-account transactions.	
2. Determine if management controls risks associated with conflicts of interest. Consider the following methods: • Making full disclosure. • Obtaining appropriate consent. • Policies against use of insider information, legal safeguards, and appropriate monitoring. • Obtaining court approval.	

Procedure	Comments
• Resolving the conflict in favor of the account beneficiaries. • Compliance with self-dealing restrictions in ERISA, Internal Revenue Code, and state laws. • Obtaining independent, reasoned legal opinions.	
Asset Management Objective: Assess the DD's policies and controls related to asset management products and activities.	
1. Determine that the board of directors, fiduciary/trust committee, or related subcommittee has approved general investment and administrative guidelines for all significant holdings in the trust function: (If the Personal Trust or the Employee Benefit Module is completed, document procedures in the reference module.)	
2. Review internal and external investment research methods and evaluate management's due diligence in selecting assets for purchase.	
3. Determine if the criteria for including or excluding assets from the approved list of investments is appropriate.	
4. Assess the process for retaining or selling assets that do not meet established investment criteria.	
5. Review methods for developing investment strategies and determine that such strategies are consistently applied.	
Retirement Accounts Objective: Assess the DD's policies and controls related to Retirement Account products and activities.	
1. Does the DD serve in a fiduciary capacity for retirement plans? If so, does the plan comply with the ERISA fiduciary requirements described in this section? *Refer to Chapter 5 of the FDIC Trust Examination Manual for additional examination considerations.*	

Procedure	Comments
2. If applicable, assess whether the DD reasonably documented investment decisions for ERISA plans, as a best practice.	

6. SECURITIES-RELATED ACTIVITIES

In the United States, the SEC is the primary regulator of securities and securities-related activities, though banking regulators like the Department and state securities regulators have authority relating to custody, bank operations and offerings.

Certain digital assets that a DD may custody or otherwise support with product and service offerings may meet the SEC's or states' definition of a security, invoking SEC or state regulation, and potential Department registration requirements.

The Investment Advisers Act of 1940, the Gramm–Leach–Bliley Act ("GLBA"), the SEC's Regulation R, and state securities laws provide several exemptions for a bank to engage in certain limited security-related activities without seeking the otherwise customary registrations with the SEC or state securities regulator. DDs interested in engaging in securities activities—either through traditional securities or digital (tokenized) securities—may elect to engage in these activities using one of the exemptions.

The Department may examine any securities-related activities of a DD, and the exemptions that the DD has relied on to engage in these activities during an examination. This section provides an overview of these regulations and exemptions. In addition, this section discusses a DD's ability to act as a "qualified custodian" for investment advisors.

6.1. When is a Digital Asset a Security?

During the offering, sale or distribution of digital assets, entities must consider whether U.S. federal and state securities laws are applicable. The applicability of the securities regulations to activities involving digital assets will depend on if the digital asset meets the definition of "security" under the Securities Exchange Act of 1933 ("The Exchange Act"), the Securities Act of Nebraska or other applicable state law. The definition of a "security" includes "investment contracts". A digital asset should be analyzed to determine whether it meets the definition of a security.

The SEC issued a framework[27] for "investment contract" analysis for digital assets. The framework highlights the U.S. Supreme Court's Howey Case, which provides clarification of what would be deemed as an "investment contract". Conducting an analysis to determine if an asset is an investment contract using this case is known as the Howey Test. Nebraska and most states have also adopted the Howey test when reviewing whether an investment is an "investment contract." The framework states that, "Under the Howey Test, an "investment contract" exists when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others." Whether a digital asset is determined to be an investment contract is based on certain facts and circumstances. The SEC framework then provides further details to the following key elements of the Howey Test:

- The investment of money
- Common Enterprise

[27] U.S. Securities and Exchange Commission (SEC) "Framework for 'Investment Contract' Analysis of Digital Assets." (April 2019)

- Reasonable Expectation of Profits Derived from the Efforts of Others

The SEC considered the question of when a digital asset is a security in its July 2017 Report on its investigation into the digital asset DAO[28], in an analysis that determined that DAO was a security.

This analysis includes the following discussion of what constitutes a security:

> Under Section 2(a)(1) of the Securities Act and Section 3(a)(10) of the Exchange Act, a security includes "an investment contract." See 15 U.S.C. §§ 77b-77c. An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. See SEC v. Edwards, 540 U.S. 389, 393 (2004); SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946); see also United Housing Found., Inc. v. Forman, 421 U.S. 837, 852-53 (1975) (The "touchstone" of an investment contract "is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."). This definition embodies a "flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits." Howey, 328 U.S. at 299 (emphasis added). The test "permits the fulfillment of the statutory purpose of compelling full and fair disclosure relative to the issuance of 'the many types of instruments that in our commercial world fall within the ordinary concept of a security.'" Id. In analyzing whether something is a security, "form should be disregarded for substance," Tcherepnin v. Knight, 389 U.S. 332, 336 (1967), "and the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto." United Housing Found., 421 U.S. at 849.

In the DAO Investigation report, the SEC then performed an analysis of history, organization, and promotion of the DAO enterprise against the criteria discussed above. The principal considerations in the SEC's analysis were the following:

- The SEC determined that participants obtained DAO tokens by making an initial investment. The SEC's analysis found this to be the case even though most of the "initial investments" were made in the form of tokens in another digital asset, the cryptocurrency Ether. Under this analysis, the form of the investment is not material. The SEC's analysis goes further to explain that an "investment" could even take the form of 'goods and services,' or some other "exchange of value."
- The SEC determined the investors who purchased DAO were investing in a "common enterprise" and reasonably expected to earn profits through that enterprise. This conclusion was supported by the promotional materials distributed by the promoters of DAO, which described profits and dividends being earned by token holders through the profits of projects funded with the proceeds of the initial investments.
- The SEC determined that the profits that the investors sought were "to be derived from the managerial efforts of others." The DAO was aligned to an organization with governance structure that provided for approval of certain actions, including the approval of projects designed to generate profits, through the voting of token owners. However, the SEC analysis

[28] U.S. Securities and Exchange Commission (SEC). "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO." (July 2017).

also found that substantial managerial control of the enterprise was also vested in the DAO token "Curators," supporting the SEC's conclusion.

The SEC and state securities regulators have taken numerous enforcement actions against digital asset companies for unregistered securities offerings and fraudulent misstatements and omissions. Senior SEC officials have publicly expressed[29] the opinion that other cryptocurrencies (notably bitcoin and ether) do not meet the definition of a security. Furthermore, federal courts have determined that bitcoin is a commodity.[30]

Though further guidance from states and the SEC may provide greater clarity, the SEC and the states, including Nebraska, have clearly state that when digital assets meet the definition of a security, security laws must be complied with. As discussed further below, when considering offering custody or other services connected to a digital asset, DDs should perform an analysis against all current guidance to identify if the asset is, or may likely be deemed, a security. The details and the results of the analysis should be documented by the DDs. DDs should also have a process in place to continually monitor the digital assets they do support for changes in applicable regulation or regulatory guidance, or the structure of asset itself, that may impact the digital asset's classification.

6.2. Investment Advice and the Investment Advisers Act of 1940

A DD that provides financial services to investment advisers or registered investment companies may be governed by applicable state and federal securities laws. The Nebraska Securities Act[31], The Investment Company Act of 1940 ("ICA") and the Investment Advisers Act of 1940 ("IAA") are the primary statutes controlling the activities of investment companies, investment advisers and their associated service providers. These statutes establish a variety of registration, reporting, and regulatory requirements on investment companies and investment advisers. Generally, the SEC is responsible for the administration, regulation, and enforcement of these statutes.

Prior to the enactment of GLBA, banks were exempt from investment adviser registration under the IAA. As a result of this exemption, many banks provided investment advisory services through unregistered internal bank divisions. Other banks made strategic decisions to provide these services through registered investment advisory bank subsidiaries or holding company affiliates. GLBA amended the IAA to require a bank to register with the SEC as an investment adviser if the bank provides investment advisory services to a registered investment company. All other investment advisory activities conducted in the bank, including investment advisory activities involving collective investment funds and other unregistered investment funds (such as private equity funds) are still exempt from federal investment adviser registration requirements.

Banks that are required to register their investment advisory services have four organizational methods available to them:

[29] Securities and Exchange Commission (SEC). "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO." (July 2017).
[30] *See, e.g.,* CFTC v. McDonnell, 287 F. Supp. 3d 213, 224–226 (E.D.N.Y. 2018).
[31] Neb. Rev. Stat. §§ 8-1101 to 8-1124

- The bank may register itself as an investment adviser.
- The bank may register a "separately identifiable department or division" (SIDD) of the bank that performs the advisory services.
- The bank may register a subsidiary that performs the advisory services.
- A holding company subsidiary or other affiliate that performs the advisory services can be registered.

Investment adviser registration will subject the bank's investment advisory activities to regulation by the SEC under the IAA unless the DD's assets under management are below $100,000, in which case, they would be subject to Department oversight.. While a bank must register its advisory function to the extent it advises a registered investment company, it may choose to consolidate some or all of its investment advisory activities in the registered entity. The investment advisory activities included in the registered investment adviser must adhere to the IAA. The IAA and the rules promulgated under the IAA regulate advertising, solicitation, and receipt of performance fees by registered investment advisers. Investment adviser registration requires the adviser to, among other things:

- Establish procedures to prevent the misuse of nonpublic information;
- Maintain certain books and records, and submit periodic information reports to the SEC;
- Supervise investment advisory firm employees;
- Comply with the general anti-fraud provisions of the federal securities laws; and
- Become statutorily disqualified from performing certain services for a mutual fund if the adviser violates the law.

6.3. Regulation R and Other Registration Exceptions

The Securities Exchange Act of 1934 ("Securities Exchange Act") requires most entities that engaged in broker-dealer activities [32] to register with the SEC. Similarly, state securities laws require entities that engage in broker-dealer activities to be registered in the state in which they transact business, unless otherwise excluded or exempt. Regulation R implements certain exceptions from registration for banks engaged in certain broker-dealer activities. The *FDIC Trust Examination Manual* [33] contains a detailed description of these exemptions and the guidance for determining compliance with them. An examiner is recommended to consult the *FDIC Manual* for a more detailed description of the exemptions. The SEC also has published [34] a summary of Regulation R. A summary of the primary exemptions available are included here:

- A networking exemption for certain compensation stemming from referrals by bank employees to a broker-dealer.
- An institutional referral exemption that permits a bank, in certain circumstances, to pay an unregistered employee a higher-than-nominal, contingent fee for the referral of an

[32] The Securities Exchange Act defines a "broker" as "any person engaged in the business of effecting transactions in securities for the account of others" and defines "dealer" as "any person engaged in the business of buying and selling securities for his own account, through a broker or otherwise."
[33] Federal Deposit Insurance Corporation (FDIC). "Trust Examination Manual." (May 2005).
[34] U.S. Securities and Exchange Commission (SEC). "Regulation R: Exceptions for Banks from the Definition of Broker in the Securities Exchange Act of 1934 — A Small Entity Compliance Guide." (August 2008).

"institutional customer" or "high net worth customer" to a broker-dealer.
- An exemption for certain trust and fiduciary activities when the bank is "chiefly compensated" for effecting securities transactions for trust and fiduciary accounts through fees which are "relationship compensation".
- An exemption for certain special accounts, transfer accounts and a de minimis number of accounts.
- An exemption for certain activities related to sweep accounts.
- An exemption for certain money market fund transactions, related to sweep activity.
- An exemption for accepting orders to effect transactions in securities from or on behalf of certain custody accounts.
- An exemption for certain transaction in securities issued pursuant to Regulation S.
- An exemption for certain securities-lending transactions.
- An exemption for certain excepted or exempted transaction in investment company securities.
- An exemption for certain transactions effected for an employee benefit plan.

Determining which digital assets are securities will be a threshold question in evaluating when a Regulation R exemption may be needed or when an exemption is met. This topic is discussed above in the subsection *6.1 "When is a Digital Asset a Security?".* Once a digital asset is determined to be a security, the existing standards, as outlined in the *FDIC Trust Examination Manual* should be generally applied.

In addition to Regulation R, Section 3(a)(4)(B) of the Exchange Act also includes other "broker" exceptions for banks. These exceptions include transactions in exempt securities (such as U.S. government securities); certain stock purchase plans; affiliate transactions; private securities offerings; identified banking products; municipal securities; and a de minimis number of other securities transactions.

While a DD may seek an exemption under any of the criteria of Regulation R and may choose which exemption to apply when multiple exemptions are available, the Department expects that the following exemptions will be most commonly applied by DDs and are therefore discussed in more detail here.

Trust & Fiduciary Activities Exception

The trust & fiduciary activities exception allows a bank, in its capacity as trustee or fiduciary, to effect securities transactions for the accounts it administers if the following conditions are satisfied:

- Transactions are affected in the bank's trust department or other department that is regularly examined by a state or federal banking regulator for compliance with fiduciary principles and standards;
- The bank does not publicly solicit brokerage business;
- The bank is "chiefly compensated[35]" for its trust and fiduciary activities on the basis of:
  - An administrative or annual fee; or

[35] The Regulation text, as well as the FDIC Trust Examination Manual, contains substantial detail defining what "chiefly compensated" means in this context, as well as defining a "chiefly compensated test."

  - A percentage of assets under management; or
  - A flat or capped per order processing fee equal to not more than the cost incurred; or
  - A combination of the above.
- Trades are affected in compliance with Exchange Act Section 3(a)(4)(C), which requires trades to be affected:
  - By a registered broker-dealer; or
  - Via a cross trade or substantially similar trade either within the bank or between the bank and an affiliated fiduciary in a manner that is not contrary to fiduciary principles; or
  - In some other manner that the SEC permits.

For the purposes of Regulation R, fiduciary capacity is defined by the Office of the Comptroller's regulation 12 C.F.R. Part 9. Fiduciary capacity includes acting as trustee, executor, administrator, registrar of stocks and bonds, transfer agent, guardian, assignee, receiver, or custodian under a uniform gift to minors act, or as an investment adviser if the bank receives a fee for its investment advice, or in any capacity in which the bank possesses investment discretion on behalf of another. The prohibition on solicitation of brokerage business restricts the extent to which a bank can advertise that it effects securities transactions.

In its advertisements, a bank may only indicate that it effects securities transactions in connection with its trust and fiduciary services. The fact that a bank effects securities transactions cannot be made more prominent that the material advertising the bank's provision of trust and fiduciary services.

The trust & fiduciary exception, as well as the other GLBA/Regulation R exceptions and exemptions, require that securities transactions be executed in accordance with the Exchange Act's execution requirements, which generally require securities transactions to be executed by a registered broker-dealer or in a cross trade. Regulation R, however, provides several exemptions from the Exchange Act's trade execution requirement. Regulation R permits banks to effect certain transactions directly through the National Securities Clearing Corporation (“NSCC”), the issuer's transfer agent, or an insurance company, if certain requirements are met.

Regulation R permits transactions in "covered securities" to be affected through the NSCC, directly with the transfer agent, or with an insurance company or separate account that is excluded from the definition of transfer agent in the Exchange Act. A "covered security" is a registered mutual fund, or a variable insurance contract funded by a separate account that is registered. The following two requirements must be satisfied:

- The security is not traded on a national securities exchange or through the facilities of a national securities association or an interdealer quotation system; and
- The security is distributed by a registered broker-dealer, or the sales charge is no more than the amount permissible for a security sold by a registered broker-dealer under Investment Company Act of 1940 rules.

Regulation R also provides an exemption whereby transactions in employer securities for employee benefit plans can be affected directly with the transfer agent provided that:

- No commission is charged;

- The transaction is solely for the benefit of an employee benefit plan account;
- The security is obtained directly from:
  - The employer; or
  - An employee benefit plan of the employer.
- The security is transferred only to:
  - The employer; or
  - An employee benefit plan of the employer.

Custody & Safekeeping Exception

The GLBA provides an exception from the definition of broker for banks that provide custody and safekeeping services. GLBA specifically provides that a bank will not be considered a broker if it engages in the following custodial and safekeeping activities:

- Providing safekeeping and custody services to customers with regard to securities, including the exercise of warrants and other rights on behalf of bank customers;
- Facilitating the transfer of funds or securities as a custodian or clearing agent in connection with the clearance and settlement of its customers' transactions in securities;
- Facilitating lending or financing transactions or investing cash in connection with its safekeeping, custody, and securities transfer services;
- Holding securities pledged by a customer to another person or securities subject to repurchase agreements involving a customer, or facilitating the pledging or transfer of such securities by book entry or as otherwise provided by law, provided that the bank maintains records separately identifying the securities and the customer; or
- Serving as a custodian or provider of other related administrative services to any individual retirement account, pension, retirement, profit sharing, bonus, thrift savings, incentive, or other similar benefit plan.

In addition to the statutory exception, Regulation R[36] provides two exemptions whereby a bank can take orders for the purchase or sale of securities from custody account customers. One exemption allows a bank, as part of its customary banking activities, to accept orders for securities transactions from employee benefit plan accounts, individual retirement accounts, and similar accounts. The second exemption allows a bank to accept orders for securities transactions from custody account customers on an accommodation basis.

The exemptions discussed below apply to accounts for which the bank acts as a custodian. Regulation R defines an account for which a bank acts as a custodian of an account that is:

- An employee benefit account;
- An individual retirement account or similar account;
- An account established by a written agreement between the bank and the customer that sets forth the terms that will govern the fees payable to, and rights and obligations of, the bank regarding the safekeeping or custody of securities; or
- An account for which the bank acts as a directed trustee.

[36] 17 C.F.R. § 247.

Whether a bank serves as custodian for securities or other assets of an account depends on the services the bank provides to the account, rather than the label used to identify the account. Thus, a bank that acts as an escrow agent or paying agent and that provides custody and safekeeping services to the account is considered an account for which the bank acts as custodian, notwithstanding the fact that the account is not called a custody or safekeeping account.

Exemption for EB, IRA, and Similar Accounts

A bank may accept orders for securities transactions from custody accounts for employee benefit ("EB") plans, individual retirement plans, and similar accounts provided that:

- The bank does not advertise that it accepts orders, except as part of advertising its other custody and safekeeping services;
- No bank employee is compensated based on whether a securities transaction is executed or on the quantity, price, or type of security involved;
- The bank is not a trustee or fiduciary, other than a directed trustee;
- The bank is not acting as a carrying broker; and
- The bank complies with the trade execution requirements in Exchange Act Section 3(a)(4)(C)(i).

Banks may not advertise that custody accounts are securities brokerage accounts or are a substitute for a brokerage account. While the bank cannot be a trustee or fiduciary and still rely on the custody exemption, there is an exception made for banks that serve as directed trustees. A bank that serves as a directed trustee is eligible for the custody exemption provided it complies with the other requirements of the exemption. A directed trustee is a trustee that does not hold any investment discretion over an account.

Within common securities industry usage, the terms "carrying broker" and "clearing broker" are virtually identical and often are used interchangeably. In certain instances, the terms mean a broker that, as part of an arrangement with a second broker (an "introducing" or "corresponding" broker), allows the second broker to be subject to lesser regulatory requirements (e.g., under the net capital provisions of Exchange Act Rule 15c3-1 and the customer protection provisions of Exchange Act Rule 15c3-3). Technically, however, a "carrying broker" is a broker that holds funds and securities on behalf of customers, whether its own customers or customers introduced by another broker-dealer, and a "clearing broker" is a member of a registered clearing agency.

The preamble to the final Regulation R discusses factors that the SEC would consider in determining if a bank were acting as a carrying broker. The SEC indicated that it would consider the existence of shared clients between a broker-dealer and bank and the reason why clients of the broker-dealer have established custody accounts at a bank. The existence of shared customers where the broker-dealer causes its customers to establish custody accounts at a bank could result in a determination that the bank was acting as a carrying broker for the broker-dealer. If, however, the clients of the broker-dealer independently decide to open a custody account at a bank, then the bank would likely not be viewed as acting as a carrying broker for the broker-dealer. Banks may share systems and platforms with a broker-dealer, for example an affiliated broker-dealer with which a common BSA/AML compliance system is used. Other examples of permissible arrangements include legal and compliance functions, accounting, and finance functions (such as

payroll and expense account reporting), and administrative functions (such as human resources and internal audit). Moreover, banks may perform limited back-office functions for a broker-dealer without being deemed as acting as a carrying broker. A broker-dealer cannot delegate to a bank functions that require registration with a self-regulatory organization ("SRO"), and the broker-dealer must retain control of its property, cash, and securities.

In addition to bank custodians, non-custodial, non-fiduciary third-party administrators and record keepers for employee benefit plans may rely on the EB/IRA custody exemption provided that:

- Both the custodian bank and the third-party administrator/record keeper comply with the requirements of the exemption; and
- The administrator/record keeper does not execute cross trades other than:
  - Crossing or netting open-end mutual funds not traded on an exchange; or
  - Crossing or netting orders for accounts held at the custodian bank that contracted with the third-party administrator/record keeper.

Exemption for Accommodation Trades

For custody accounts that are not maintained by an employee benefit plan, individual retirement accounts, or other similar accounts, a bank may accept orders for securities transactions as an accommodation to the customer provided:

- Any fee charged or received by the bank does not vary based on:
  - Whether the bank accepted the order; or
  - The quantity or price of the securities bought or sold.
- Advertisements do not state that the bank accepts orders for securities transactions;
- Sales literature does not state that the bank accepts orders, except as part of describing other aspects of its custodial and safekeeping services;
- The bank does not provide investment advice or research, make recommendations, or solicit transactions. However, the bank may:
  - Advertise or provide sales literature as allowed in the exemption;
  - Respond to customer inquiries about custody and safekeeping services by providing:
    - Advertisements and sales literature;
    - Prospectus or sales literature prepared by a registered investment company; or
    - Materials based on the above.
- The bank complies with the compensation and trade execution requirements of the EB/IRA exemption.

The requirement that the bank not provide investment advice or research, make recommendations, or solicit transactions does not prohibit a bank from cross marketing its trust and fiduciary services to custody account customers. Banks may cross-market investment advisory services to custody customers by:

- Providing non-account specific information via newsletters, websites, etc.;
- Providing examples of research, including stock specific research that the bank provides to other persons for marketing purposes.

A bank, however, may not provide personalized investment research regarding securities held in a custody account. Lists and menus of securities that can be purchased or sold are not considered investment advice.

If a customer has both a trust or fiduciary account and a custody account at the bank, the bank may provide investment advice and research to the customer in connection with the trust or fiduciary account. The bank is not responsible for how the trust or fiduciary accountholder uses such advice or research.

Sub-custodians

A bank that acts as a sub-custodian for an account for which another bank acts as custodian may rely on either the EB/IRA exemption or the Accommodation Trade exemption, depending on the type of account at the custodial bank, provided that:

- Both the sub-custodian and the custodian bank comply with the requirements of the respective exemption; and
- The sub-custodian does not execute cross trades, other than:
  - Crossing or netting open-end mutual funds not traded on an exchange; or
  - Crossing or netting orders for accounts of the custodian.

Applicability to the DD

The above sections outline the various exemptions that can be relied upon by banks under Regulation R and other registration exemptions. However, some of the listed transactions and activities may not be applicable to the DD's business and allowed as permissible activities under the Nebraska Financial Innovation Act.

6.4. Compliance with GLBA and Regulation R

Regardless of the GLBA exception or Regulation R exemption, which is relied on by the DD, the Department expects each DD to conduct a comprehensive analysis of its securities activities to ensure compliance with the GLBA and Regulation R, and to maintain records to demonstrate compliance. A DD's comprehensive plan and implementation of actions to address GLBA and Regulation R requirements should be tailored commensurate with the scope and complexity of a DD's securities activities. Ongoing processes should be established to ensure effective compliance with the GLBA, Regulation R, and record-keeping requirements. A DD's compliance should address the following, as applicable:

- Include all affected DD units in the planning and implementation processes, such as the various impacted business lines, human resources, legal, compliance, internal audit, risk management, finance, operations, and marketing.
- Understand the nature of the activities and revenues generated.
- Analyze DD and employee compensation related to securities activities.
- Make decisions on which GLBA exception or Regulation R exemption is to be used for

preserving the DD's securities activities.
- Determine whether certain accounts or business lines need to be re-priced, restructured, or pushed out to a broker-dealer.
- Review customer disclosures.
- Review advertising policies and procedures.
- Review securities trade order handling.
- Develop business line policies and procedures.
- Make necessary programming changes to affected systems.
- Develop risk control programs that include compliance, risk management, and internal audit functions to ensure ongoing monitoring and testing.
- Develop record-keeping systems to demonstrate compliance.
- Provide DD employee training.
- Incorporate the GLBA and Regulation R requirements in the DD's review and approval processes as appropriate. Such processes may include review of new products and services, marketing materials, customer disclosures, and employee compensation.

DD managers who do not effectively implement and monitor compliance with the GLBA and Regulation R or maintain records demonstrating compliance with these requirements expose the DD to compliance, reputation, strategic, and operational risks.

Noncompliance with these requirements could present potential legal issues that may include enforcement actions by the SEC, the Department, or other state securities regulators. Additionally, a DD's failure to comply with broker registration requirements or exceptions from broker registration could trigger customer rescission of a contract that potentially could lead to DD indemnification of customer losses. Section 29(b) of the Securities Exchange Act includes a provision that every contract made in violation of the Securities Exchange Act or of any rule or regulation adopted under the Securities Exchange Act, with certain exceptions, shall be void. Regulation R (Rule 780) includes an exemption for banks from liability under section 29 of the Securities Exchange Act that addresses inadvertent Regulation R compliance failures by banks that could otherwise trigger rescission of contracts between a bank and a customer.

6.5. Antifraud Provisions

DDs operating securities custody services and sales programs should be aware that they remain liable under the antifraud provisions of the federal and state securities laws and regulations (section 10(b) of the Securities Exchange Act, Securities Exchange Act Rule 10b-5, and Section 8-1102 of the Securities Act of Nebraska) even if their securities transaction and custody activities comply with an exception or exemption from broker-dealer registration. These antifraud provisions prohibit materially false and misleading representations or omissions in connection with the purchase or sale of securities. Securities sales activities should be designed to minimize the possibility of customer confusion and to safeguard DDs from liability under the antifraud provisions of the federal and state securities laws and regulations. DDs must ensure clients are not misled or provided inaccurate representations about the nature of and risks associated with the securities they facilitate the sale of. This includes making an untrue statement of material fact or omitting to state a material fact necessary in order to make the statement made, in light of the circumstances under which they were made, not misleading. Securities Exchange Act rule 10b-5

and similar state laws are specific to the antifraud provisions of purchasing and selling securities whether or not the securities or transaction were exempt from registration.

Sellers could face potential liability under these antifraud provisions for making materially false and misleading statements and omissions in connection with offers and sales of securities. Safe and sound DD practices also require that DD or third-party related sales activities be operated to avoid customer confusion about the products being offered. Use of affiliated or unaffiliated third parties to sell securities does not relieve DD management of the responsibility to take reasonable steps to ensure that the sales activities meet the requirements under the antifraud provisions.

6.6. The Custody Rule

The Custody Rule under the Investment Advisers Act of 1940 requires investment advisors that hold custody of client funds or securities to maintain those assets with qualified custodians.[37] The term "qualified custodian" is defined under the custody rule amendments under the Investment Advisers Act of 1940 to include any "bank"[38] defined as:

"'Bank' means (A) a banking institution organized under the laws of the United States or a Federal savings association, as defined in section 2(5) of the Home Owners' Loan Act, (B) a member bank of the Federal Reserve System, (C) any other banking institution, savings association, as defined in section 2(4) of the Home Owners' Loan Act, or trust company, whether incorporated or not, doing business under the laws of any State or of the United States, a substantial portion of the business of which consists of receiving deposits or exercising fiduciary powers similar to those permitted to national banks under the authority of the Comptroller of the Currency, and which is supervised and examined by State or Federal authority having supervision over banks or savings associations, and which is not operated for the purpose of evading the provisions of this title, and (D) a receiver, conservator, or other liquidating agent of any institution or firm included in clauses (A), (B), or (C) of this paragraph."

The DD would be required to meet the definition of a "bank", in order to be considered a "qualified custodian".

The Custody Rule imposes several requirements on SEC-registered investment advisers to protect client funds and securities over which the adviser has custody. These are[39]:

- Use of "qualified custodians" to hold client assets. With certain limited exceptions, an investment adviser is required to maintain client funds and securities with a "qualified custodian." Qualified custodians can be banks, registered broker-dealers, futures commission merchants, or certain foreign entities. A qualified custodian either maintains client funds and securities in a separate account for each client under that client's name, or in accounts that contain only client funds and securities under the name of the investment adviser as agent or trustee for the clients.

[37] 17 C.F.R. § 275.206(4)-2.
[38] 15 USC § 80b-2(a)(2)
[39] U.S. Securities and Exchange Commission (SEC). "Investor Bulletin: Custody of Your Investment Assets." (March 2013).

- Notices to clients detailing how their assets are being held. If the investment adviser opens the custodial account, it must notify clients in writing of the qualified custodian's name, address, and the manner in which the funds or securities are maintained, promptly when the account is opened and following any changes to this information. Also, in any account statement sent by the adviser, the adviser must advise its clients to compare account statements sent by the adviser with the account statements sent by the custodian.

- Account statements for clients detailing their holdings. Investment advisers must have a reasonable basis to believe that the qualified custodians that maintain client funds and securities send account statements at least quarterly to the adviser's clients directly. This permits advisory clients to compare the statements they receive from the custodian with any statements or other information they receive from their adviser and to determine whether account transactions, including deductions to pay advisory fees, are proper.

- Annual surprise exams. If the investment adviser has custody of client assets, it must enter into a written agreement with an independent public accountant to examine those assets on a surprise basis every year. The accountant performing the "surprise" examination will contact some, or all, advisory clients to confirm their holdings with those listed on the records of the adviser. An adviser that has custody solely because it has the authority to deduct advisory fees from client accounts is not required to obtain a surprise examination.

- Additional protections when a related qualified custodian is used. If the custodian is also the investment adviser or is affiliated with the adviser in some way, the adviser must, among other things, obtain a report from the related qualified custodian that includes an opinion of an independent public accountant regarding the effectiveness of the custodian's procedures for safeguarding client funds and securities every year. Pursuant to the Nebraska Banking Act[39], financial institutions are required to enter into an agreement with a public accountant to conduct an examination pursuant to the requirements of 17 C.F.R. 275.206(4)-2(a)(4) and (6). Additionally, an adviser that uses a related qualified custodian is itself subject to annual surprise exams, as described in the preceding paragraph.

6.7. The Customer Protection Rule

A DD may wish to custody assets, including digital assets, for a broker-dealer. The broker-dealer must comply with financial responsibility rules including, as applicable, the custodial requirements of Rule 15c3-3 under the Securities Exchange Act of 1934, commonly known as the Customer Protection Rule.

The SEC and FINRA has issued a joint statement discussing the application of this rule to digital assets custodians. As the joint statement explains, "the purpose of the Customer Protection Rule is to safeguard customer securities and funds held by a broker-dealer, to prevent investor loss or harm in the event of a broker-dealer's failure, and to enhance the Commission's ability to monitor and prevent unsound business practices. Put simply, the Customer Protection Rule requires broker-dealers to safeguard customer assets and to keep customer assets separate from the firm's assets, thus increasing the likelihood that customers' securities and cash can be returned to them in the

[39] Neb. Stat. § 8-1, 141 (LB649, 2021)

event of the broker-dealer's failure […] Among its core protections for customers, Rule 15c3-3 requires a broker-dealer to physically hold customers' fully paid and excess margin securities or maintain them free of lien at a good control location."

The joint statement goes on to explain the unique challenges presented by applying the Customer Protection Rule to digital assets: "In particular, a broker-dealer may face challenges in determining that it, or its third-party custodian, maintains custody of digital asset securities. If, for example, the broker-dealer holds a private key, it may be able to transfer such securities reflected on the blockchain or distributed ledger. However, the fact that a broker-dealer (or its third-party custodian) maintains the private key may not be sufficient evidence by itself that the broker-dealer has exclusive control of the digital asset security (e.g., it may not be able to demonstrate that no other party has a copy of the private key and could transfer the digital asset security without the broker-dealer's consent). In addition, the fact that the broker-dealer (or custodian) holds the private key may not be sufficient to allow it to reverse or cancel mistaken or unauthorized transactions. These risks could cause securities customers to suffer losses, with corresponding liabilities for the broker-dealer, imperiling the firm, its customers, and other creditors." [41]

Because a DD may make an application to become a member bank of the Federal Reserve System, the DD may meet the definition of "bank" under the Exchange Act and thus be eligible to serve as a "good control location" under the Customer Protection Rule.

The SEC issued another statement[42], regarding the custody of digital asset securities by broker-dealers in order to encourage innovation around the application of Securities Exchange Act Rule 15c3-3 to digital asset securities. Within the statement the SEC sets forth that for a period of five years[43], that the broker-dealer will not be subject to a Commission enforcement action if they meet all criteria that is outlined within the statement. The statement would be applicable to a broker-dealer that deems itself to have obtained and maintained physical possession or control of customer fully paid and excess margin digital asset securities for the purposes of paragraph (b)(1) of Rule 15c3-3.

To comply with the statement, a broker dealer would be required meet the following criteria:

1. "The broker-dealer has access to the digital asset securities and the capability to transfer them on the associated distributed ledger technology;
2. The broker-dealer limits its business to dealing in, effecting transactions in, maintaining custody of, and/or operating an alternative trading system for digital asset securities; provided a broker-dealer may hold proprietary positions in traditional securities solely for the purposes of meeting the firm's minimum net capital requirements under Rule 15c3-

[41] U.S Securities and Exchange Commission (SEC)-Financial Industry Regulatory Authority (FINRA). "Joint Staff Statement on Broker-Dealer Custody of Digital Assets" (July 2019).
[42] U.S Securities and Exchange Commission (SEC) "Custody of Digital Asset Securities by Special Purpose Broker-Dealers" (December 2020)
[43] Five years from the date of the publication of the SEC statement "Custody of Digital Asset Securities by Special Purpose Broker-Dealers" (December 2020)

1[44], or hedging the risks of its proprietary positions in traditional securities and digital asset securities.

3. The broker-dealer establishes, maintains, and enforces reasonably designed written policies and procedures to conduct and document an analysis of whether a particular digital asset is a security offered and sold pursuant to an effective registration statement or an available exemption from registration, and whether the broker-dealer meets its requirements to comply with the federal securities laws with respect to effecting transactions in the digital asset security, before undertaking to effect transactions in and maintain custody of the digital asset security;
4. The broker-dealer establishes, maintains, and enforces reasonably designed written policies and procedures to conduct and document an assessment of the characteristics of a digital asset security's distributed ledger technology and associated network prior to undertaking to maintain custody of the digital asset security and at reasonable intervals thereafter;
5. The broker-dealer does not undertake to maintain custody of a digital asset security if the firm is aware of any material security or operational problems or weaknesses with the distributed ledger technology and associated network used to access and transfer the digital asset security, or is aware of other material risks posed to the broker-dealer's business by the digital asset security;
6. The broker-dealer establishes, maintains, and enforces reasonably designed written policies, procedures, and controls that are consistent with industry best practices to demonstrate the broker-dealer has exclusive control over the digital asset securities it holds in custody and to protect against the theft, loss, and unauthorized and accidental use of the private keys necessary to access and transfer the digital asset securities the broker-dealer holds in custody;
7. The broker-dealer establishes, maintains, and enforces reasonably designed written policies, procedures, and arrangements to:
    i. specifically identify, in advance, the steps it will take in the wake of certain events that could affect the firm's custody of the digital asset securities, including, without limitation, blockchain malfunctions, 51% attacks, hard forks, or airdrops;
    ii. allow for the broker-dealer to comply with a court-ordered freeze or seizure; and
    iii. allow for the transfer of the digital asset securities held by the broker-dealer to another special purpose broker-dealer, a trustee, receiver, liquidator, or person performing a similar function, or to another appropriate person, in the event the broker-dealer can no longer continue as a going concern and self-liquidates or is subject to a formal bankruptcy, receivership, liquidation, or similar proceeding;
8. The broker-dealer provides written disclosures to prospective customers:
    i. that the firm is deeming itself to be in possession or control of digital asset securities held for the customer for the purposes of paragraph (b)(1) of Rule 15c3-3 based on its compliance with this Commission position; and

[44] 17 CFR. 240.15c3-1

ii. about the risks of investing in or holding digital asset securities that, at a minimum: (a) prominently disclose that digital asset securities may not be "securities" as defined in SIPA—and in particular, digital asset securities that are "investment contracts" under the Howey test but are not registered with the Commission are excluded from SIPA's definition of "securities"—and thus the protections afforded to securities customers under SIPA may not apply; (b) describe the risks of fraud, manipulation, theft, and loss associated with digital asset securities; (c) describe the risks relating to valuation, price volatility, and liquidity associated with digital asset securities; and (d) describe, at a high level that would not compromise any security protocols, the processes, software and hardware systems, and any other formats or systems utilized by the broker-dealer to create, store, or use the broker-dealer's private keys and protect them from loss, theft, or unauthorized or accidental use[44]; and

9. The broker-dealer enters into a written agreement with each customer that sets forth the terms and conditions with respect to receiving, purchasing, holding, safekeeping, selling, transferring, exchanging, custodying, liquidating and otherwise transacting in digital asset securities on behalf of the customer.[45]"

Further clarification and details surrounding the applicable criteria can be found within the SEC statement published on December 23, 2020.

6.8. SEC Staff Accounting Bulletin

The SEC also issued Staff Account Bulletin ("SAB") 121 to provide staff interpretation and interpretive guidance regarding the accounting obligations to safeguard crypto-assets an entity holds for platform users. The SAB is applicable to entities that file reports pursuant to Sections 13(a) or 15(d) of the Securities Exchange Act of 1934 ("Exchange Act") and entities that have submitted or filed a registration statement under the Securities Act of 1933 ("Securities Act") or the Exchange Act that is not yet effective. It is also applicable entities subject to Regulation A and private operating companies that file financial statements with the SEC.

The SAB highlights three main risks related to crypto assets including technology risk, legal risk, and regulatory risks. The SAB provides facts and circumstances of an outlined scenario related to the securing of crypto assets by an entity and then provides three questions and interpretive responses for each question. The information provided within the SAB provides interpretive guidance for entities to mitigate associated risks safeguarding crypto assets. The main points from the SAB are the following:

- If an entity is safeguarding crypto assets, including maintaining the cryptographic key information, then a liability should be present on its balance sheet to reflect the entities obligation to safeguard the crypto assets for its platform users.

[44] The broker-dealer will need to retain these written disclosures in accordance with the broker-dealer record retention rule. See 17 CFR 240.17a-4(b)(4)

[45] The broker-dealer will need to retain these written agreements in accordance with the broker-dealer record retention rule. See 17 CFR 240.17a-4(b)(7)

- The entity should also recognize an asset at the same time that it recognizes the safeguarding liability.
- The liability and asset should be measured at the initial recognition and each reporting date at fair value of the crypto assets.
- Notes should be made to the entity's financial statements that include clear disclosures of the nature and amount of the crypto-assets the entity is responsible for holding for users, with a separate disclosure for each significant crypto-asset, and the vulnerabilities.
- The entity would also need to disclose in the footnotes of its financial statements regarding the fair value measurements for the crypto assets as well as the accounting of liabilities and assets.
- The SAB also outlines how and when entities should apply the guidance included in the SAB on its financial statements based on the entities filing and registration requirements

6.9. Examination Procedures

Procedure	Comments
Digital Assets as Securities Objective: Assess the DD's compliance with SEC registration requirements regarding digital assets meeting the definition of a security.	
1. Evaluate if the DD has a sufficient process to review digital assets involved in new product offerings to determine if the asset may meet the SEC's definition of a security. Determine if this process is reasonably documented.	
2. Evaluate if the DD has a sufficient process in place to monitor each of the digital assets supported by the DD for changes that might affect the classification of the digital assets as a security.	
3. Does the DD currently offer custody or other services that meet the SEC's definition of a security? If so, does the DD have the requisite SEC registrations (or exemptions) necessary to conduct the business offerings connected with these digital assets?	
GLBA or Regulation R Exemptions or Exceptions Objective: If applicable, ensure the DD is properly relying on the necessary exemption not be deemed a registered broker.	

Procedure	Comments
1. Does the DD rely on GLBA or Regulation R exemptions or exceptions? If so, determine: • What exemption or exception is being relied on. • Ensure the DD is properly applying the correct exemption or exception.	
The Custody Rule Objective: Assess the DD's compliance with SEC's Custody Rule.	
1. Does the DD act as a qualified custodian to an investment advisor? If so, determine whether: • The DD meets the definition of a qualified custodian. • The investment advisor's client's funds are segregated by client or aggregated into a single account under the investment adviser's name as agent or trustee for the clients. • Statements are sent directly to the investment advisor's clients at least quarterly. • If the investment adviser is arranging for an annual surprise examination. Has a surprise examination been scheduled during the past year for each investment advisor DD client? • The DD is affiliated with any investment advisor for whom it holds assets If so, has the DD obtained an opinion of an independent public accountant regarding the effectiveness of the custodian's procedures for safeguarding client funds and securities?	
The Customer Protection Rule Objective: Assess the DD's Compliance with SEC's Customer Protection Rule	
1. Does the DD custody digital asset securities? If so, determine whether: • The DD incorporated requirement SEA rule 15c3-3 into its procedures and controls. If so, determine whether the controls are reasonably designed to comply with the rule requirements • The DD assets are separated from customer assets. • The DD has reasonable procedures and controls to safeguard customers' digital asset securities.	

Procedure	Comments
• The DD has a process in place to readily return customer securities to the customer, in the event of the DD's failure. • The DD has procedures and controls in place regarding recordkeeping and financial reporting. • The DD incorporates any of the controls outlined within SEC statement "Custody of Digital Asset Securities by Special Purpose Broker Dealers" as a best practice	
SEC Staff Accounting Bulletin No. 121 Objective: Determine if the DD incorporated the criteria from the SEC Staff Accounting Bulletin (SAB) No. 121.	
1. Determine if the DD is an entity that the SAB would be applicable to, as outlined within the SAB. If so, ensure the DD has incorporated the necessary financial and disclosure criteria on their financial books and records.	
2. If SAB is not applicable to the DD, determine whether the DD incorporated the financial and disclosure criteria outlined within the SAB as a best practice.	

7. CUSTODY SERVICES

7.1. Overview

As previously mentioned, the NFIA specifies that a DD is authorized to provide digital asset and cryptocurrency custody services.[47] Additionally, DDs may issue stablecoins, carry on a nonlending digital asset banking business for customers, and provide payment services upon request of a customer. Finally, though prohibited from fiat currency lending, a DD may facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to, controllable electronic record exchange, staking, controllable electronic record lending, and controllable electronic record borrowing.[48] Examples of other facilitation activities may include trading or exchanging of digital assets as well as providing sub-custodian services.

The SEC[49] has provided examples to help clarify when certain arrangements constitute a custody relationship. In the context of investment advisers, under the SEC's custody rule:

- The first example clarifies that an adviser has custody when it has possession of client funds or securities, even briefly. An adviser that holds clients' stock certificates or cash, even temporarily, puts those assets at risk of misuse or loss. The amendments, however, expressly exclude inadvertent receipt by the adviser of client funds or securities, so long as the adviser returns them to the sender within three business days of receiving them. The rule does not permit advisers to forward clients' funds and securities without having "custody," although advisers may certainly assist clients in such matters. In addition, the amendments clarify that an adviser's possession of a check drawn by the client and made payable to a third party is not possession of client funds for purposes of the custody definition.

- The second example clarifies that an adviser has custody if it has the authority to withdraw funds or securities from a client's account. An adviser with power of attorney to sign checks on a client's behalf, to withdraw funds or securities from a client's account, or to dispose of client funds or securities for any purpose other than authorized trading has access to the client's assets. Similarly, an adviser authorized to deduct advisory fees or other expenses directly from a client's account has access to, and therefore has custody of, the client funds and securities in that account. These advisers might not have possession of client assets, but they have the authority to obtain possession.

- The third example clarifies that an adviser has custody if it acts in any capacity that gives the adviser legal ownership of, or access to, the client funds or securities. One common instance is a firm that acts as both general partner and investment adviser to a limited partnership. By virtue of its position as general partner, the adviser generally has authority to dispose of funds and securities in the limited partnership's account and thus has custody of client assets.

[47] Neb. Rev. Stat. § 8-3024(1) (LB707, 2022)
[48] Neb. Rev. Stat. § 8-3005 (LB707, 2022)
[49] SEC Release No. IA-2176 "Custody of Funds or Securities of Clients by Investment Advisors"

A DD may custody assets in segregated accounts or in an omnibus account provided that the omnibus account contains only customer assets under the DD's name as agent or trustee for customers. The DD may similarly offer custody arrangements which maintain digital assets under a bailment as a fungible or nonfungible asset. The DD should maintain exclusive control over all assets while in custody. The meaning and significance of "exclusive control" is discussed in a subsection below.

A DD is expected to enter into a written custody agreement with its custody clients clearly setting forth the roles and responsibilities, in understandable language, of the custodian and customer, the terms and conditions of the custodial relationship, and what authorities the client wishes for the custodian to exercise over the assets. Specific considerations that may be addressed in a custody agreement include:

- If the assets are to be maintained in a segregated or omnibus account;
  If the assets are to be maintained under a bailment as a nonfungible or fungible asset;
- What activities are prohibited (e.g., demand deposits and loans);
- Necessary disclosures to customers including, but not limited to, the schedule of fees and charges;
- Acknowledgement that the digital asset deposits are not insured by Federal Deposit Insurance Corporation;
- The terms and conditions of facilitating digital asset lending (refer to Asset Lending in Section 10);
- What, if any, discretionary actions the DD may take on the customer's behalf;
- The safekeeping of the digital assets, including but not limited to, the handling of private keys;
- Source code version handling;
  Applicable laws; and
- Liens

7.3 Custody Agreements subsection discusses this topic in further detail.

A DD may wish to outsource all or part of their custody operations to a third-party sub-custodian. While such arrangements are not prohibited, these arrangements should not result in the application of weakened standards to those required by the Department or applicable federal law. The management of sub-custodial relationships is discussed further in *7.5. Sub-Custody Relationship* section below.

7.2. Exclusive Control or Possession

A DD is required to safeguard digital assets under custody. Custodied digital assets are those which are under the control of the DD, with "control" as defined in the NFIA[50] whereby the DD has *exclusive power* to effect or prevent a transfer of assets. Exclusive power can exist even if "the person has agreed to share the power with another person." The Director has the final authority to

[50] Neb. Stat. § 8-3003 (LB649, 2021)

determine whether DDs demonstrate exclusive power in a particular type of custodial arrangement.

A DD is definitionally required[51] to maintain control or possession (as applicable based on the asset) over digital assets, including digital (tokenized) securities, under custody. While the customer retains legal rights, and in the case of a bailment legal title, to an asset custodied by an DD, the DD must maintain the exclusive ability to effect on-ledger transfers of an asset while in custody.

By the nature of digital assets, knowledge of the private key is the only requirement needed to perform immutable on-ledger transactions. Conversely, on-ledger transactions cannot be performed without knowledge of the private key, even if ownership can be readily established, and there is generally no central authority to step into remedy transaction errors, thefts, or lost keys.

While knowledge of private key(s) controlling an asset custodied by the DD may be clearly established, validating that no other party has sufficient knowledge of the key(s) sufficient to effect an on-ledger transfer is, generally, impossible. The SEC and FINRA has considered this topic in their joint statement, writing: "[…] however, the fact that a broker-dealer (or its third party custodian) maintains the private key may not be sufficient evidence by itself that the broker-dealer has exclusive control of the digital asset security (e.g., it may not be able to demonstrate that no other party has a copy of the private key and could transfer the digital asset security without the broker-dealer's consent)."[52]

The Department stipulates that a custodian will have exclusive control or possession of an asset if it alone, and no other party, to a substantial degree of certainty,[53] has the ability to effect an on-ledger transfer of the asset and can readily identify such ability. Conversely, maintaining exclusive "negative control" (ability to prevent a transaction), and being able to readily identify as having negative control, is also required. A bad actor who obtains negative control can lock the customer's funds and blackmail the customer and custodian into paying them to approve transactions.

It is the Department's view that a DD establishes exclusive control or possession, as applicable, based on a holistic analysis of the following factors on a facts-and-circumstances basis:

(1) The DD possesses sufficient private key material to effect or prevent[54] an on-ledger transaction without approval or coordination from another key holder.

---

[51] See NFIA Section 8-3003(3) for the definition of "control" in the context of a digital asset in custody. There is no custody without control. As such, by definition, DDs are required to maintain control of digital assets under custody and the aforementioned subdivision can be used to determine whether the requirement to control has been met.

[52] U.S Securities and Exchange Commission (SEC)-Financial Industry Regulatory Authority (FINRA). "Joint Staff Statement on Broker-Dealer Custody of Digital Assets" (July 2019).

[53] For instance, employees of the Depository Trust and Clearing Corporation (DTCC) have access credentials that would theoretically enable them to effect transfers of securities outside normal channels. DTCC has processes and procedures in place to mitigate this potential risk. In many ways therefore, "exclusive control or possession" is a facts-and-circumstances assessment that requires high certainty, not complete verifiable certainty (which is also not present in securities markets today). The standards set forth above for digital securities are likely a higher standard of certainty relating to exclusive possession or control than those present in securities markets today.

[54] Subject to the sharing exception under NFIA Section 8-3003(3)(b)(ii)

(2) Whether the DD creates new private keys for assets under custody, or merely provides safekeeping services for customer-generated private keys.

(3) Whether the DD uses code-reviewed software, including smart contracts, to generate private keys without DD employee access, if new keys are created under (2) above.

(4) Whether interacting with or moving private keys to hot wallets is similarly restricted to code-reviewed software without DD employee access, including smart contracts.

(5) Whether DD employees have access to clear-text private keys at any stage of the custody process.

(6) Whether the DD has policies and procedures in place governing private key generation designed to prevent DD employee access and which appropriately addresses the role of: (a) private key software-related development by DD employees; and (b) information technology staff access in the case of operational failures or errors.

(7) Whether new private keys are created at the time a digital asset is returned to the customer and the method in which the asset is returned, or whether the DD returns the private key used by the DD.

(8) The overall internal control framework relied upon by the DD is tailored to ensure that no non-DD person has knowledge of private keying material sufficient to effect or impede an on-ledger transaction.

These factors may be verified by an internal or external audit or regulatory examination, consistent with traditional securities and commodities market practices.

7.3. Custody Agreements

The terms of the relationship between the DD as a custodian and its customer is established through the use of custody agreements. If a DD is providing fiduciary or other discretionary services, a separate agreement may be necessary, or may be rolled into a master agreement. These agreements form the basis of the custodial relationship and should be drafted in a way that very clearly articulates the roles and responsibilities of the parties and specifies applicable law, among other crucial factors. Standardized contracts should be employed whenever possible.

The NFIA[55] requires that the terms and conditions of a customer's digital asset depository account at a DD be disclosed to the customer at the time the customer contracts for digital asset business service. Agreement to segregate customer assets from DD assets, is of course a must, as well as an agreement to provide appropriate recordkeeping relating to customer assets, as required by Nebraska and federal law. These and other terms and conditions governing the custodial relationship should be contained in the custody agreement. Other essential components of a custody agreement include:

[55] Neb. Stat. § 8-3008 (LB649, 2021)

- The types of transactions that a customer can direct the custodian to facilitate (e.g., buying, selling, engaging in proof of stake pools, digital asset lending, etc.) or execute (e.g., permissible transactions involving stablecoins issued by the DD) to take on the customer's behalf, and the protocols for doing so;
- The conditions or scope of authority under which transactions may take place;
- Whether the assets are to be custodied under a bailment on a fungible or nonfungible basis or in an omnibus account (likely to be the case for accounts with greater transaction volumes);
- The agreement should clearly establish the requisite legal relationship between the custodian DD and the customer, including choice of law and venue, waivers of litigation in other states, liens, and issues relating to control and possessory security interests;
- The extent, if any, of the DD's discretionary and fiduciary responsibilities to the client;
- The nature of the safekeeping arrangement; particularly if the assets will be held in a segregated or omnibus account;
- Terms and conditions of facilitating digital asset lending through a third-party provider;
- Whether the DD can place liens against the custodial assets;
- The notice period required to move custodial assets to another institution and/or terminate the custody relationship;
- Source code, fork, and airdrop treatment;
- The terms of any cash management service, including requirements of deposits and any restrictions on withdrawals, particularly on short notice;
- The terms governing any sub-custody relationships that might be applicable to the customer's assets. Terms might:
    - Require that each sub-custodian assumes the same standard of care as the custodial relationship between the DD and customer;
    - Require that each sub-custodian be a "qualified custodian" or "eligible foreign sub-custodian" under the Investment Company Act of 1940;
    - Require the DD to monitor each sub-custodian and notify the customer of any material change in these or other associated risks; and
    - Require that the DD withdraw customer assets from the sub-custodian as soon as practicable and deposit them with an alternative sub-custodian if the DD believes that there has been a material increase in the risk profile of the sub-custodian; and
- The steps that the DD is obligated to take on a periodic basis to ensure that the customer's assets are being held consistent with the DD's policies and procedures, and the terms set out in the customer agreement. This may include reporting to the client the results of annual or quarterly certifications or audits, including those required by the SEC Custody Rule.

Account Statements and Disclosures

Each DD is required to provide customer account statements and disclosures consistent with best practices for custodial and fiduciary principles.

DDs are expected to provide account statements and disclosures to customers consistent with the SEC Custody Rule[56], irrespective of whether the assets are securities or subject to the Custody

[56] 17 C.F.R. § 275.206(4)-2

Rule. Nebraska Statute § 8-3008 establishes the following standards:

- A schedule of fees and charges the digital asset depository may assess, the manner by which fees and charges will be calculated if they are not set in advance and disclosed, and the timing of the fees and charges;
- A statement that the customer's digital asset depository account is not protected by the Federal Deposit Insurance Corporation;
- A statement whether there is support for forked networks of each digital asset;
- A statement that investment in digital assets is volatile and subject to market loss;
- A statement that investment in digital assets may result in total loss of value;
- A statement that legal, legislative, and regulatory changes may impair the value of digital assets;
- A statement that customers should perform research before investing in digital assets;
- A statement that transfers of digital assets are irrevocable, if applicable;
- A statement how liability for an unauthorized, mistaken, or accidental transfer shall be apportioned;
- A statement that digital assets are not legal tender in any jurisdiction;
- A statement that digital assets may be subject to cyber theft or theft and become unrecoverable;
- A statement about who maintains control, ownership, and access to any private key related to a digital assets customer's digital asset account; and
- A statement that losing private key information may result in permanent total loss of access to digital assets.

A DD should also meet the following requirements for statements, disclosures, and notifications:

- Account statements are sent by the DD to customers at least monthly, identifying the amount of funds in the customer's account and all traditional and digital assets in the customer's account at the end of the period and setting forth all transactions in the accounts during that period;
- If the DD uses consolidated account statements, then the DD must establish and maintain reasonably designed agreements, processes, and controls to ensure customer assets are accurately and correctly reflected;
- Notification of the custodian's name, address, and the manner in which the funds and assets are maintained, promptly when the account is opened and following any changes to this information;
- Source code, airdrop and fork and other subsidiary and ancillary value disclosures;
- Valuation of assets for each digital asset type, including the method used to create the valuation;
- Disclose all service level agreements for custodial services to customers;
- Disclose its responsibilities with respect to valuation of assets, providing recordkeeping, reporting services, risk measurement and compliance monitoring; and
- Other statements required by Nebraska or federal law.

Nebraska Revised Statute §8-3005(6) also states that DD shall maintain and update a public file and any internet website it maintains to include specific information about its efforts to meet

community needs, including:

- The collection and reporting of data;
- Its policies and procedures for accepting and responding to consumer complaints; and
- Its efforts to assist with financial literacy or personal finance programs to increase knowledge and skills of Nebraska students in areas such as budgeting, credit, checking and savings accounts, loans, stocks, and insurance.

7.4. Best Execution of Transactions

DDs should ensure that any third parties used to facilitate transactions on behalf of customers seek best execution of those transactions and are capable of such. Best execution standards may vary somewhat in the digital asset markets from traditional standards because of liquidity, settlement processes and other factors, but DDs should generally consider traditional asset best execution standards as the default position when evaluating third parties, absent specific compelling circumstances. If a DD is also providing fiduciary or discretionary services to a customer, higher standards may apply. In addition to evaluating third party trading processes, DDs should ensure that third parties have controls to protect against free ride transactions, as outlined in OCC Banking Circular 275.

7.5. Sub-Custody Relationships

A DD may wish to enter into a sub-custody arrangement with another financial institution as an external provider of domestic or global custody services. A DD should have a due diligence process in place for selection of this provider. Considerations of a potential sub-custodian should include:

- Financial condition.
- Position in the market.
- Annual Report on Policies and Procedures (SSAE 16).
- Availability of sufficient MIS to allow the DD to monitor its securities, cash, and income positions.
- Reporting options for the DD's customer accounts.
- The extent of the provider's sub-custodian network.
- The provider's due diligence review process for its sub-custodian DDs, and the frequency of its ongoing reviews.
- Compliance with SEC Rule 17f, when applicable.
- The provider's multi-currency accounting and reporting capabilities.
- Prohibition of any non-custodial activity except facilitation activities, which are allowable per Nebraska Revised Statute § 8-3005(2)(b) and which are explicitly permitted and governed by a contract with the DD
- Fees.

The DD should ensure that proper controls are in place for sending instructions to its custodian. In addition, the DD should have policies in place requiring that cash and asset positions be reconciled regularly. The DD should also monitor MIS reports to ensure that exception items (such as failed securities transactions and nonreceipt of income) are promptly investigated and resolved.

Given the evolving nature and standards of digital asset custody across regulatory regimes, the Department should be consulted on and approve the use of sub-custody relationships. The Department's review will be based on the analysis of the considerations listed above, as well is if the proposed sub-custodian adheres to practices and applies standards of safekeeping and risk management consistent with those applicable to Nebraska DDs as set forth in the state legislation and other best practices.

7.6. Retirement Plans

A DD providing custody for retirement plan assets may have additional duties under ERISA. ERISA's implications in the custody services area include:

- The DOL approved a class exemption relating to foreign exchange transactions of employee benefit plans. Prohibited Transaction Exemption (PTE) 98-54 is a class exemption that permits certain foreign exchange transactions between employee benefit plans and certain banks and broker-dealers that are parties in interest with respect to such plans, pursuant to standing instructions from an independent fiduciary of the plan.
- In *Harris Trust v. Salomon Smith Barney*, 530 U.S. 238 (2000), the Supreme Court held that section 502(a)(3) authorizes a "participant, beneficiary, or fiduciary" of a plan to bring a civil action against a nonfiduciary "party in interest" to redress violations of ERISA. Refer to this decision for further information.
- The DOL also issued class exemptions relating to securities lending in ERISA accounts. See *Asset Lending*.

Laws or regulations of other countries may also apply to the custodian or the sub-custodian when pension assets of another country are held in custody.

7.7. Examination Procedures

Procedure	Comments
Custody Agreements Objective: Review and assess the DD's use of custody agreements.	
1. Review the custody agreements used by the DD. Evaluate if the DD has clear, appropriate custody agreements, consistent with the principles described in this section. Discuss any ambiguities or unclear provisions with the DD's chief legal officer, chief compliance officer or general counsel.	
2. Evaluate if the DD has an appropriate process for providing account statements to customers, consistent with the principles described in this section. If the DD uses consolidated account statements, evaluate whether the controls and processes surrounding the creation and dissemination of the account statements are reasonably designed to ensure that customers' assets are accurately reflected.	
3. Evaluate if the DD makes appropriate customer disclosures, as described in this section, including with respect to source code, forks, airdrops, other subsidiary and ancillary value and other relevant factors.	
4. Review any customer complaints related to custody services provided by the DD and note whether the complaints are isolated issues or reflect broader trends that may be reflective of deficiencies.	
5. Ensure that custody agreements do not allow for any activity which is not permissible under the NFIA. Any activity for which permissibility is unclear, and/or which appears to create risks which are not appropriate for a Nebraska DD, should be escalated to the Director for further review.	
Best Trade Execution Objective: If applicable, assess the DD's approach to best trade execution.	

Procedure	Comments
1. If applicable, evaluate if the DD has a trade execution policy and program, based generally on best practices for best execution. If the DD is using a third party to execute trades, the DD should ensure that the third party has an adequate best execution practice. The practice should include, but not be limited to, analyzing pricing/valuation, counterparty selection, speed of execution, certainty of execution, counterparty risk, security practices, conflicts of interest, recordkeeping capabilities, commission rate or spread and other applicable factors. Consider whether the DD ensured that the third party has implemented higher execution standards for fiduciary accounts or as otherwise required by customer agreements or applicable law.	
2. If applicable, determine the extent to which variations or departures from traditional best execution standards may have been warranted based on the characteristics of digital assets.	
3. Evaluate and review any customer complaints related to the execution of transactions on behalf of customers.	
Sub-custodial Arrangements Objective: Assess the DD's sub-custodial relationships and governing agreements.	

Procedure	Comments
1. Determine if the DD uses any sub-custodians. If so, evaluate the sub-custodial relationship against the factors described in this section. Verify that all sub-custodial relationships have been approved by the Department and that sub-custody agreements are clear and substantially contain the same terms as required for custody agreements. Note any special dispensations or indemnifications given to sub-custodians by the custodian.	
Retirement Plans Objective: Assess the DD's compliance with ERISA guidelines.	
1. If the DD is the custodian of retirement plan assets, determine whether the DD's process for receiving 12(b)(1) fees, shareholder servicer fees, or other fees is in compliance with ERISA guidelines. See Frost and Aetna letters (DOL Advisory Opinions 97-15A and 97-16A).	
Shareholder Communication Rules Objective: Assess the DD's compliance with shareholder communication rules.	
1. SEC Rules 17 CFR 240.14-17 govern the distribution of proxy materials and the disclosure of information about shareholders whose securities are registered in a bank nominee name. • Determine the process used by the DD to code accounts (OBO or NOBO) to pass information received from issuers, such as proxies and annual reports, to beneficial owners as appropriate (17 CFR 240.14c-2 and 17 CFR 240.14c-101). • Review DD responses to requests for information from issuers to determine whether the responses were appropriate and timely (17 CFR 240.14b-2(b)). U.S. Investment Company Assets — 17 CFR 240.17f If the DD is the custodian of investment company assets, determine whether the	

Procedure	Comments
processes to comply with SEC revised rule 17f-5 and new rule 17f-7 are adequate.	
Free Riding — Regulation U — 12 CFR 221 Objective: If applicable, review the DD's compliance with Regulation U.	
1. If applicable, evaluate the DD's processes governing free riding. (Refer to OCC Banking Circular 275, "Free Riding in Custody Accounts.")	
2. If the DD is using a third party to conduct or execute trades, the DD should ensure that the third party has an adequate process to supervise and remediate free-ride violations.	
Bank Secrecy Act — 12 CFR 21.21 and 31 CFR 103 Objective: Assess if a deeper review of BSA/AML topics is necessary.	
1. Review the extent of the custody services compliance review of BSA. If a BSA review of custody services needs to be performed, refer to the Department's *DD BSA/AML and OFAC Examination Manual* and the "*Bank Secrecy Act/Anti- Money Laundering" booklet of the Comptroller's Handbook*.	

8. SAFEKEEPING AND SETTLEMENT

The custody business developed from safekeeping and settlement services provided to customers for a fee. Banks originally provided only basic safekeeping services for their customers. Although banks routinely settled trades and processed income for their own investments, their customers had to clip their own coupons, collect dividends, and take their securities out of safekeeping to settle trades or for bond maturities. Realizing that their expertise in securities processing and their image as a safe repository would be valuable to their customers, banks began to promote their securities processing ability.

The custody industry has grown to global proportions but has maintained a low profile. Custodians have been instrumental in consolidating holdings and providing expertise for a wide variety of assets held by its customers. Global custodians control trillions of dollars in assets in offices around the world.

Given the growth of use and ownership of digital assets in the 2010's and the unique risks associated with holding these assets (e.g., digital theft or loss), there has been substantial demand for safekeeping services for digital assets. With certain exceptions (e.g., cash management and foreign exchange) that apply to all activities of a DD, this section addresses traditional securities custody operations. Further information on digital asset-specific standards on these issues is provided in the following section.

8.1. Safekeeping of Custody Assets

A DD is responsible for maintaining the safety of custody assets held in physical form at one of the custodian's premises, a sub-custodian facility, or an outside depository. A custodian's accounting records, and internal controls should ensure that assets of each custody account are kept separate from the assets of the custodian and maintained under joint control. If a DD holds assets off-premises, then it must maintain adequate safeguards and controls and comply with applicable law.

8.2. On-Premises Custody of Securities

The G-30 marketplace settlement goal of T+1 will make it virtually impossible for custodians to hold marketable securities in physical form. A custodian will not be able to remove a certificate from a vault and ensure delivery to the broker in time for settlement. However, non-depository-eligible securities and miscellaneous assets (e.g., jewelry, art, coins) must be kept in physical form by a custodian. When a DD custodian holds assets in physical form in its vault, the DD should provide for security devices consistent with applicable law and sound custodial management. The custodian should have appropriate lighting, alarms, and other physical security controls. Vault control procedures should ensure segregation of custody assets from DD assets, dual control over custody assets, maintenance of records evidencing access to the vault, and proper asset transfers.

Assets should only be out of the vault when the custodian receives or delivers the assets following purchases, sales, deposits, distributions, corporate actions, or maturities. Securities movement and control records should detail all asset movements, deposits, and withdrawals, including temporary withdrawals. The vault record should include the initials of the joint custodians, the date of vault

transactions, description and amounts of assets, identity of the affected accounts, and the reasons that assets are withdrawn.

Some custodians monitor their physical vault asset movement by using a computerized securities movement and control (SMAC) system which records the actual location of off-premises assets and monitors the movement of an asset during purchase, sale, or lending.

Global custodians having offices in foreign countries or using sub-custodians should develop processes to ensure that the operations at those sites have proper internal controls to protect assets. Refer to the sub-custodian section of this manual for more information.

8.3. Off-Premises Custody of Securities

Changes in the marketplace and the large volume of securities traded each day have permanently altered the landscape of the custody world. The vast majority of custodial assets are held in book entry form. The major depositories in the United States are the Federal Reserve (for government securities) and the Depository Trust and Clearing Corporation (DTCC) (for equity and debt securities other than U.S. government securities). Currently, Euroclear and Clearstream (formerly Cedel) are two major international depositories. Each country will have at least one central securities depository (CSD) such as DTCC in the United States. Mergers and consolidations of depositories are occurring regularly to streamline global securities processing. Custodians must be ready to adapt to the rapid evolution of the securities processing world with sound internal controls to safeguard assets.

If a DD custodian uses a depository, then the DD should use SSAE 16 reports or third-party audits whenever possible to ensure that an adequate control environment exists and that the depository has established sound safeguards.

Custodians should establish strong risk-based internal controls to protect assets held off-premises. Internal controls may be either active or passive. Active controls require dual control over the authorization of all transaction information prior to data entry. Passive controls are detective or reactive in nature. Passive controls may include independent reconcilements, overdraft reports, and failed trade reports.

Custodians should reconcile changes in the depository's position each day that a change in the position occurs, as well as completing a full-position reconcilement at least monthly. Depository position changes are generally the results of trade settlements, free deliveries (assets transferred off the depository position when no cash is received), and free receipts (assets being deposited or transferred to the depository position for new accounts when no cash is paid out). When controls on free deliveries are passive, personnel independent of the free delivery and free receipt asset movement process should reconcile changes in daily positions. If applicable, independent personnel should reconcile the depository's position report to the custodian's accounting system each month. Exceptions noted in the control systems should be reported to management in a timely manner.

Electronic terminal interfaces used to effect depository withdrawals, affirm trades, and deliver instructions to a depository should be subject to appropriate access controls (ID and password) and

periodic audits. Each person with electronic terminal interface access should have a separate ID and password and should be able to perform only functions necessary for their job. IDs should not be shared. The person (normally the system administrator) responsible for granting access to the system that interfaces with a depository should be independent of the securities processing activity.

Job profiles should be developed for each job or position that needs to use system functions. The profile should contain a detailed description of the job and the reason system access is needed. The profile description should also outline those functions and systems that must be considered incompatible responsibilities in order to keep duties properly separated. A security procedure in the system administration process should monitor ID changes and ID issuance to ensure that duties remain properly separated. Such a procedure ensures, for example, that a reconciler could not move assets from a depository and then certify that the system is in balance.

8.4. Safekeeping and Settlement of Securities Transactions

The risks associated with securities settlement will only increase as the securities markets become truly global. New technologies allow for faster movement of money from market to market. New and different securities products are being developed that require custodians to know the basic investment characteristics of each type of security they handle. Managing the risk of global securities settlement is a key to successful custody operations.

Basics of Securities Settlement

The DD may use a third party to facilitate security trades for DD customers. The securities settlement process contains some element of risk at each stage of the transaction. A third party must make sure that it effectively manages each process in the transaction: trade initiation, trade affirmation, trade settlement, and trade compliance. The third party and DD should use rapid and accurate communication among all participants to reduce the likelihood of a failed trade or loss.

The trading environment and securities settlement cycles are constantly undergoing changes to reduce risk and take advantage of technological developments. Trade settlement standards are moving to T (same day trade) or T+1 from the three-day (T+3) settlement standard for U.S. equities. U.S. government securities and other U.S. domestic fixed income trades generally settle in a T or T+1 trading cycle. The shortening of the settlement period reduces a counterparty's credit risk and market risk in price-sensitive securities.

Trade Initiation

Transactions to buy or sell securities are initiated in a variety of ways. DD custody customers may deliver buy or sell instructions to the DD or third party by phone or online. Some customers may place trades with their broker at the third party and inform the custodian of the terms of the trade by phone, or electronic terminal. In some cases, the customer, usually through an investment advisor, will place the trade with the broker and affirm the trade with the depository. In this case the DD custodian will receive instructions for settlement of the trade from the depository or settling agent. The third party and/or DD should have a process in place to ensure that a customer's instructions are clear, arrive in an agreed- upon format, and are properly documented (by electronic

instruction, recorded phone line, fax, or in writing). The date the trade is executed is known as the trade date and is referred to as "T" or T+0.

Trade Affirmation/Confirmation

The trade affirmation/confirmation process occurs when a depository forwards the selling broker's confirmation of the transaction to the buyer's custodian. The executing third party reviews the trade instructions from the depository and matches the information to instructions for the trade received from the customer. If the instructions match, the executing third party affirms the trade. If the instructions do not match, then the executing third party or custodian will "DK" (don't know or reject) the trade or will instruct the selling broker how to handle the mismatch. The affirmation/confirmation process is generally completed by T+1 in a normal T+3 settlement cycle. On day T+2, depositories usually send settlement instructions to the custodian after affirmation and prior to settlement date. The instructions contain the details of the trade that has been affirmed and agreed to by the parties in the trade. Custodians will match the settlement instructions to their records and prepare instructions to their wire department to send funds or expect funds from the depository on T+3 of the settlement cycle. If an issue or error has been identified during this process, the custodian will take necessary steps with the executing third party to promptly correct the settlement or trade error.

Trade Settlement

Trade settlement occurs when securities and money are moved to complete the trade. Settlement occurs on T+3 in a T+3 settlement cycle. The depository sends a settlement report to all participants on the activities for their account. The custodian and third party should review and reconcile the depository's settlement report to its activity report each day that asset positions change at the depository. The custodian should also compare the cash movement activity in its deposit account with its daily cash accounting control records. The custodian and third parties should have a process to reconcile the changes in the depository position each day and should perform a full position reconcilement at least monthly.

Trade Compliance

Trade compliance is the internal control process used by custodians to manage trade transactions. In this process, the custodian determines that the customer's account has the securities on hand to deliver for sales, that the customer's account has adequate cash or forecasted cash for purchases, that trades are properly matched or marked as "Don't Know" ("DK"), and that the depository's settlement instructions agree with the custodian's SMAC system. A third-party using a properly executed trade compliance system may prevent failed trades and needless reversals of transactions.

A third-party's trade compliance system should be able to detect free-riding attempts. A financial institution that permits freeriding may violate Regulation U (12CFR 221), may aid, and abet violations of Regulation X (12 CFR 224) or Regulation T (12 CFR 220), and may assume the risk that it will be unable to recover from the customer the funds advanced to settle a transaction.

The Future of Securities Settlement

The basics of settlement as previously outlined will have to change to meet industry needs and lower risk in the system. Third parties utilized by the DD lacking a forward-looking technology strategy may find themselves at a competitive disadvantage.

Third parties utilized by the DD that offer trading services should develop strategies that use new technology to address risk and the T+1 or shorter settlement cycle.

Third parties should assess their technological readiness now to maintain a competitive position. Straight-through processing (STP), electronic trade confirmation (ETC), and standing instruction databases (SID) are technological processes designed to facilitate the future of domestic and global securities settlement. The goal of STP and T+1 is to minimize operational risk in trade processing. Custodians that do not develop technology strategies for custody services may be faced with trying to outsource trade settlement operations.

International Securities Trade Settlement

The same basic settlement process applies whether the transaction is domestic or international. However, each foreign market has different exchanges, regulations, and settlement conventions. These differences present risks that custodians must consider and address. It is essential that a sub-custodian has in-depth market knowledge. Additional issues that must be considered when trading international securities include:

- Legal and regulatory framework.
- Currency or capital controls.
- Registration of securities [56].
- In-country processing (trading and custody) requirements.
  - Local market conventions, such as:
  - Settlement cycle.
  - Use of central securities depository.
  - Availability of delivery versus payment in the market.
  - Methods of payment (real-time gross settlement, net settlement, central bank accounts, checks).
  - Degree of automation.
  - Trade execution.
  - Trade affirmation/confirmation process.
  - Delivery and safekeeping of securities (physical vs. book-entry).
- Different currencies used for settlement.
- Whether the custodian offers contractual settlement.
- Taxation.

[56] Many countries limit by percent the foreign ownership of their domestic securities. This creates a "dual" local and foreign market, which may cause problems by delaying registration of the beneficial ownership. The result may be a price difference between foreign and local shares. Issues may arise related to lost income, corporate actions, securities sales, and securities lending.

- Local reporting obligations.

Third parties and the DD should have a process in place to identify applicable laws and monitor compliance with laws of the countries in which they may be settling transactions. DD custodians should attempt to use depositories and sub-custodians that provide DVP settlement for all cross-border trades.

Executing third parties may choose to provide contractual settlement to the customers in some markets as a competitive strategy. In contractual settlement, the customer is credited with the sale proceeds on the contractual settlement date regardless of whether the proceeds have been received. Conversely, even if purchased securities are not received, the customer's account is debited on the contractual settlement date. The DD and third party should manage the risk of offering contractual settlement by incorporating in the agreement an understanding that if a transaction does not settle in an agreed- upon time, the transaction will be unwound.

8.5. Cash Management

Cash management is a service provided to customers involving moving, managing, and monitoring cash positions associated with securities transactions. Cash management responsibilities should be clearly defined in the custody contract or a separate agreement.

8.6. Foreign Exchange

The DD may provide foreign exchange ("FX") services through a third party to facilitate settlement of cross-border securities transactions. The custody agreement should state the terms and conditions of using a third party for foreign currency transactions, either by transaction or through the use of standing instructions. If the standing instructions do not direct the custodian to execute an FX transaction or a forward transaction, the customer should accept the risk of currency fluctuations prior to settlement. Foreign exchange services may also be used to facilitate a customer's currency hedging activities at a third party. For further information on foreign currency transactions, Refer to the *"Risk Management of Financial Derivatives" booklet of the Comptroller's Handbook*.

When standing instructions are used for an ERISA account, and the transactions are executed through the custodian's foreign exchange desk, special restrictions may apply. Prohibited Transaction Exemption (PTE) 98- 54, issued by the Department of Labor on November 13, 1998, granted a class exemption for custodians using their own foreign exchange desks to execute foreign currency transactions pursuant to standing instructions.

8.7. Reporting and Recordkeeping

An important part of any custodian's business strategy is to provide its customers with recordkeeping and reporting services. The recordkeeping services should meet the customers' specialized needs and comply with applicable recordkeeping and reporting laws and regulations. Custodians should be able to generate customized customer reports as well as required regulatory and legal reports.

Custody customers have different reporting needs ranging from only quarterly reports to real-time on-line access. Some customers, especially those involved in mutual fund management, may need customized daily reports of their activity in domestic stocks and bonds, foreign securities, derivatives, options, or other unusual investments. Customers may also require multicurrency recordkeeping and reporting capabilities. The custodian may need to develop customized reporting systems to deliver reports for custody customers. These systems may include Internet access, dial-up access, and on-line trading terminals. DD and third parties should carefully review their customers' reporting and recordkeeping requirements to ensure that they have the systems capability to provide the necessary services in an adequate manner.

Recordkeeping requirements for custodians extend beyond the normal requirements for tax reporting and financial accounting. DDs are required to maintain records in connection with the Bank Secrecy Act; recordkeeping and confirmation requirements for securities transactions, as required by 12 CFR 12, and other applicable laws related to record retention.

Custodians offering services in foreign countries must also observe the recordkeeping and reporting requirements of those countries.

Reporting and recordkeeping systems are important risk management tools. A DD's custody systems should provide activity and exception reports that allow management to effectively identify and monitor the risks in its custody operations.

When standing instructions are used for an ERISA account, and the transactions are executed through the custodian's FX desk, special restrictions may apply. Prohibited Transaction Exemption (PTE) 98- 54, issued by the DOL on November 13, 1998, granted a class exemption for custodians using their own FX desks to execute foreign currency transactions pursuant to standing instructions.

8.8. Examination Procedures

Procedure	Comments
Safekeeping of Custody Assets Objective: Assess the DD's policies, practices, and controls for the safekeeping of digital assets.	
1. Determine whether any further review of the safekeeping process is needed after reviewing the audit and control processes related to on- premises and off-premises safekeeping. Consider: • The scope of the audit coverage. • The size and nature (age) of exceptions reported. • Charge-offs due to lost or stolen securities.	

Procedure	Comments
2. For global custody activities, determine whether the DD performs effective due diligence before entering a market. Consider: • Country risk. • The settlement environment. • Restrictions on foreign investment. • Investability of the market. • Availability and integrity of financial information. • Ability to perform services profitably. • Payment systems risk.	
3. Determine whether the DD's due diligence process for selecting a global sub-custodian or third party is appropriate. Consider whether: • The DD performed a review of the institution's financial strength and its insurance coverage. • The DD reviews the sub-custodian's or third parties' position in and knowledge of the local market. • The DD determined that the sub-custodian or third party has an adequate internal control environment. • The DD determined that the sub-custodian or third party has an appropriate level of automation, and its plans for future systems development are adequate. • The quality and experience of the personnel were evaluated. • The global custodian is ensuring that the sub-custodian is complying with SEC Rule 17f in cases when the sub-custodian holds assets of a U.S. mutual fund.	

Procedure	Comments
Settlement Objective: Ensure the DD has policies and controls in place to assess a third party's transaction settlement processes	
1. Determine if the DD has policies and controls in place for the handling of trade settlements. Consider whether: • The DD is allowed to accept trade instructions for customers directly. If so, assess whether the process for accepting trade instructions is reasonably designed. • If applicable, ensure proper trade instructions are received. • If applicable, trade instructions are properly documented. • If applicable, ensure trade instructions were promptly forwarded to facilitate the trade through the third party • Failed trades or trade errors are monitored. • Confirmation sent by the DD or third party are sent as required and contain all necessary data. • Customer accounts are monitored to determine that the securities or cash needed for settlement are available. • Information and instructions from the depository agree with the custodian's securities movement and control system (SMAC). • Ensure settlements are DVP. • Review for any customer complaints the DD received from a customer related to trade settlement or trade error	
2. The DD should have policies and controls for cross-border trades and foreign exchange services at the third-party trade facilitator. Areas to consider would be: • FX and forward contract instructions for each trade or per standing	

Procedure	Comments
instructions. • Indemnity for FX risk when the customer does not want to use FX or forward contracts.	
Asset Servicing Objective: To determine the effectiveness of the processes designed to ensure effective and efficient servicing of assets in custody.	
1. Evaluate the income collection process based upon a review of the following: • The methods and services subscribed to that provide information (or forecasts) on income from custody assets (look closely into irregular payments such as asset-backed securities). • The internal control process, including maps, suspense accounts, and the suspense account monitoring and control process for processing income payments. • The process for aging items in the income suspense accounts. (Review for possible unclaimed property or escheatment issues.) • Whether income payments are contractual or actual. • The process for monitoring, verifying, and posting reinvested income •	
2. The DD has reasonable processes and controls in place for the creation and delivery of tax documents and handling foreign asset tax reclaims. Areas to consider: • Review the systems used for customer tax documents and tax reporting. • Determine if the DD maintains tax records as required by federal and state laws.	

Procedure	Comments
• Determine if the DD ensures customer tax documents are delivered timely • Determine whether the process for addressing tax reclaims on foreign assets or securities is appropriate. • Determine if the DD obtains updated information from foreign tax authorities. • Determine if the DD effectively manages language differences. • Determine if the DD monitors the statute of limitations on filing tax reclaims. • Determine if the DD effectively manages the length of time required to obtain refunds (some countries process reclaims only once per year). • If applicable, determine if the tax document and reporting process considers FX transactions and applicable foreign taxes • Review customer complaints related to tax issues • Determine if the DD requires that claims be filed for individual/beneficial owners rather than for commingled/omnibus accounts.	
Cash Management Objective: Assess the DD's policies, practices, and controls for cash and funds management.	
1. Evaluate the DDs procedures and processes for managing customer funds. Determine if these comply with Legislative Bill 649 (2021) and the Nebraska Financial Innovation Act.	
2. Review any complaints received by the DD related to the management of customer funds.	

Procedure	Comments
Recordkeeping Objective: Assess the DD's compliance with recordkeeping requirements.	
1. Determine whether internal controls provide for accurate and reliable record keeping and regulatory reporting. Consider the extent to which the DD's record keeping systems: • Maintain records in sufficient detail to properly reflect all DD activities. • Report the assets of each account separately from the assets of every other account. • Account separately for principal and income in accordance with governing trust account agreements. • Facilitate the timely and accurate processing of all DD department transactions. • Provide for accurate filing of the required periodic regulatory financial reports. • Demonstrate compliance with the SEC/FRB Regulation R and GLBA broker exception rules, in particular with the "Chiefly Compensated" requirement of the Trust & Fiduciary Exception. • Provide for accurate and timely reporting of cost basis information on Form 1099, as well as the provision and receipt of transfer statements. (See IRC §6045 and §6045A)	
2. Determine that adequate reconciliation procedures are in place, including but not limited to internal accounts, and cash management services.	

9. SAFEKEEPING OF DIGITAL ASSETS

9.1. Private Key and Seed Management

Most digital assets (such as Bitcoin and Ethereum) utilize distributed ledger technology ("DLT"). Distributed ledgers in turn rely on public key infrastructure ("PKI") to implement strong authentication and digital signatures. PKI involves assigning addresses and public and private keys to digital asset users, which are then used in protocols to execute and validate transactions. In a digital asset transaction, a private key is used to digitally sign a transaction, while the associated public key is used to validate the signature and transaction. In this design, knowledge of the private key provides the ability to transfer a digital asset. Thus, any individual with knowledge of a user's private key can sign transactions and thus has effective control of the associated digital assets. Per the Office of the Comptroller of the Currency, "a bank that provides custody for cryptocurrency in a non-fiduciary capacity would essentially provide safekeeping for the cryptographic key that allows for control and transfer of the customer's cryptocurrency."[58]

Unlike most payment systems within the traditional financial system, digital asset transactions effectuated using DLT are typically irreversible. Due to the nature of digital assets, DDs must provide safekeeping for all the private keys associated with the addresses where their customers' digital assets are held and maintain exclusive control or possession over these keys. DDs providing custody services for digital assets must implement policies, procedures, and programs to ensure digital assets are securely created, stored, and maintained to ensure uninterrupted availability.

If the private key is lost, the digital asset is effectively worthless as it can no longer be spent, withdrawn, or transferred.

9.2. Digital Asset Wallets and Private Key/Seed Storage

Digital asset wallets are mechanisms for storing public and private key pairs, which may involve software and/or hardware solutions, as well as external services. Digital asset wallets often offer functionality to sign transactions using the private key(s) and provide a user access to their digital assets. Digital asset transactions are typically recorded in their associated public distributed ledger. Digital asset wallets can be connected to the internet (often referred to as a "hot wallet") or stored offline (often referred to as a "cold wallet" or as "cold storage"). Forms of cold storage can include printing private keys or seeds onto paper or other mediums such as steel, as well as storing private keys in specialized hardware that stores private keys offline. By their design, hot and cold wallets offer tradeoffs between transaction latency (i.e., the time required to access the private keys and sign transactions) and security from malicious third parties (i.e., holding digital assets offline to mitigate the risk of cyber-attack). All else equal, online or "hot wallets" have greater third-party cybersecurity risk of theft, due to the vulnerabilities of being connected to the internet and vulnerabilities of the IT network on which they reside. For additional information on cyber security risks see the *DD Information Security Examination Manual*.

[58] Office of the Comptroller of the Currency "Interpretive Letter #1170" (July 22, 2020).

Cold wallets may be vulnerable to cyberattack when they are brought online in order to execute a transaction. Cyber-attacks have also been conducted against air-gapped networks in some circumstances. Also, cold wallets may require human intervention when they are brought online, which introduces increased operational risk associated with human error or internal theft of private keys. Additionally, a cold storage signing scheme may rely on some form of business logic (held in an online server) to compel the cold wallet to sign transactions; in this scheme if the business logic is compromised, the cold wallet itself would in effect be compromised though in practice, the private keys / seeds may have not been exposed. Lastly, certain approaches to cold storage (such as the use of hardware security modules ["HSM"]) may be less adaptable to changes in blockchain protocols than hot wallets. HSMs qualify as a method of cold storage, however.

Irrespective of the digital asset wallet type that is used, it is important that DDs implement controls to ensure appropriate digital asset transactions and safekeeping from internal and external threats. DDs should recognize the threats posed by external cyber-attacks, internal theft and by human operators, and implement mitigating controls. There are many digital asset wallet products that aim to mitigate these risks while optimizing the tradeoffs between transaction latency and security. These solutions are sometimes marketed under the labels of "nearline" or "warm storage", and typically involve additional software, hardware and/or policy controls. Whatever digital asset wallet type(s) used by the DD (for each digital asset), a DD shall demonstrate its ability to manage the same level of compliance related to safekeeping, recording and transaction handling.

Each digital asset (or, more precisely, the blockchain or digital ledgers that support them) may be implemented using distinct PKI algorithms. Moreover, each asset may update its protocols sporadically and independently. Thus, each digital asset may require a unique digital asset wallet solution in order to sign transactions. DDs should confirm and monitor their compliance with the protocols they need to support each digital asset for which they provide custody services for. DDs should also be aware that products offering additional layers of wallet security may only support certain digital asset protocols and may be incompatible with updates to the digital asset protocols.

Due to the heightened risks associated with online digital asset wallets, DDs should only maintain private keys in hot storage which are necessary to conduct customer transactions. The mechanism and thresholds for transfer between hot, cold, and other forms of storage must be well documented and subject to rigorous internal controls and auditing. To ensure sufficient liquidity and the protection of customer assets, a DD should be able to execute a withdrawal of all digital assets in a timely manner. Additionally, the customer private key storage policy should require that the majority of customer private keys not required for customer transactions should be held in risk appropriate storage to mitigate against losses arising from malicious computer intrusion or computer failure.

DDs should have the following standards in place. Accordingly, examiners should assess the degree to which the DD's systems, documentation, and processes adhere to these standards, and identify potential gaps:

- The DD has in place mechanisms to assess its liquidity needs, including primary and secondary appropriately denominated assets and/or sums required for the execution of transactions in order to inform its private key storage policy so that the policy is consistent and supports the DD's operations.

- The private keys associated with the majority of assets under custody not required for customer transactions are held in cold storage to mitigate against losses arising from malicious computer intrusion or computer failure.
- The DD only maintains private keys in hot storage which are necessary to conduct customer transactions.
- The DD has documentation, internal controls and audit procedures relating to its mechanisms and thresholds in place to facilitate the transfer between hot, cold, and other forms of storage.
- The DD has the ability to execute a withdrawal of all digital assets in a timely manner in order to provide liquidity and protect customer assets.
- The DD has in place insurance or other forms of risk mitigation, and these mitigants inform its private key storage policy.
- The DD demonstrates the ability to manage the same level of compliance related to safekeeping, recording and transaction handling for each digital asset it provides custody services for.

9.3. Deterministic Wallets and Private Key / Seed Phrase Generation

Many digital asset wallets (known as "deterministic wallets") generate private and public key pairs from a "seed" which is sometimes stored as a list of mnemonic words. Seeds can be used to derive all of the private keys associated with the digital asset wallet for which it was generated. Seeds can therefore be thought of as similar to a master key for a digital asset wallet. Thus, if the user loses access to their digital asset wallet, knowledge of the seed may provide a way to regain access to the wallet and the associated digital assets. Since seeds can be used to generate private keys, it is important that DDs apply the same or higher security standards to seeds that they do for private keys. In circumstances where DDs use mnemonic seed phrases, the phrase must be broken up into at least two or more parts and DDs should ensure that a sufficient number of backup seed phrases that could be used to facilitate a transaction are not stored within any single point of access.

Hierarchical deterministic wallets (also known as "HD wallets") are a form of deterministic wallets that can generate many "child" public/private key pairs from a "parent" key that itself is generated from a known seed. The use of hierarchical deterministic wallets has the potential to reduce the operational risks associated with managing large sets of private/public key pairs since HD wallets allow many public/private key pairs to be generated from a single known seed.

A DD may generate a new wallet address for each transaction to ensure a customer's privacy, security, and confidentiality. Before adopting such a policy, a DD shall consider potential business cases where traceability of address activity is desirable, especially to ensure compliance with federal customer identification, anti-money laundering and beneficial ownership requirements. While it is not required, DDs may use hierarchical deterministic wallets to operationalize this approach.

DDs that use deterministic wallets and generate seeds should ensure they are created using a National Institute of Standards and Technology ("NIST") compliant deterministic random bit generator, secure non-deterministic key generation mechanism, or other method approved by the Director. For additional information on cyber security risks, see the *DD Information Security Examination Manual*.

9.4. Digital Asset Custody Models [Omnibus versus Segregated Accounts]

DDs may custody customers' digital assets in a separate account for each customer under that customer's name (known as a "segregated account") or place digital assets in an omnibus account if permitted by the customer. In circumstances where the DD maintains a separate custody account for each customer, the DD must provide safekeeping for each private key and seed associated with each customer's account. If a DD aggregates customers' custodied digital assets in an omnibus account, the account must contain only customer digital assets under the DD's name as agent or trustee for customers. Details of the account structure may be explicitly agreed upon by the DD and a customer or contained in the customer agreement. The DD must provide safekeeping for all of the private keys and seeds associated with omnibus custody accounts and provide customers with clear notice that custody services may not result in the digital assets of the customer being strictly segregated from other customer assets.

There are advantages and disadvantages to both the segregated account and the omnibus account models. The omnibus account model enables fewer complex operations compared to the segregated account model which can reduce operational risks and costs. However, the pooling of digital assets into an omnibus account can also create, "a centralized 'honey pot' that may attract internal or external theft or cybersecurity attacks."[59] Additionally, under the omnibus account model, customers may face higher insolvency risk in the event of the insolvency of the custodian since the customers are, "not recorded on chain as the owner."[60] The omnibus account model also requires robust record-keeping mechanics in order to manage and record ownership off-chain.

Conversely, due to the complexity associated with managing a higher volume of customer accounts, the segregated account model typically has higher costs and operational risks when compared to the omnibus account model.[61] All else equal, the segregated account model may offer greater protection from internal and external theft and cybersecurity attacks since customer assets are controlled by distinct private keys and a breach of one account should not compromise the security of other accounts that have not been directly targeted. However, if private keys or seeds for customers' accounts are stored in a centralized location, it is possible that a single security breach could compromise many segregated customer accounts.

9.5. Private Key/Seed Management Risk Factors

Digital asset custodians face a number of risks associated with key management and digital asset safekeeping including operational failure, the theft or loss of private keys, the co-mingling of customer assets, and inaccurate record-keeping.[62]

[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] Board of the International Organization of Securities Commission. "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms" (February 2020).

Operational Failure

Digital asset custodians may lose access to private keys or seeds due to operational failure. Operational failure can occur due to hardware failure, software bugs, signing protocol vulnerabilities, cyberattack or other events that result in the loss or compromise access to private keys or seeds of customer accounts.

Unauthorized Access and Use of Private Keys or Seeds

Digital asset custodians face risks associated with the unauthorized access and use of private keys/seeds from internal malicious actors as well as from external parties. Internal malicious actors with knowledge of private keys/seeds or access to the systems required to initiate transactions may execute unauthorized transactions. External third parties also pose a risk to DDs and may seek to obtain access to private keys or seeds through cyberattack or other means.

Inaccurate Record Keeping and Manipulation of Logs/Audit Files

Digital asset custodians may fail to reconcile records or properly account for assets. The risk of record keeping errors or inaccuracies is particularly pronounced in the circumstance the custodian uses omnibus accounts for the custody of customer assets.

Failure to maintain accurate records may also weaken or compromise protection of customer assets in the event of a receivership or other contingency.

9.6. Private Key/Seed Management Risk Mitigation

Digital asset custodians should implement policies, procedures, and programs to mitigate the risks associated with digital asset custody. To ensure compliance and a safe and secure key management approach, DDs should deploy technical and operational key management controls and safeguards to secure and limit access to custodied private keys and seeds. Since each digital asset may use a different underlying blockchain with unique features and protocols, distinct approaches and solutions may be needed to optimize private key/seed management for each digital asset a DD provides custody services for. Additionally, DDs may deploy combinations of multiple safeguards and controls to optimize the management and security of their customers' private keys and seeds.

9.7. Approaches to Private Key/Seed Management

Digital asset custodians may deploy a number of hardware and software solutions (in conjunction with various transaction signing schemas) in order to enhance security, increase flexibility, limit access or to develop and deploy workflows to execute digital asset transactions. DD examiners should understand the technical solutions deployed by the DD for key management and how the solutions fit into the DD's overall key management and digital asset custody strategy. The approaches listed below may be utilized by DDs and may be deployed in conjunction with one another.

Hardware Security Modules

A hardware security module (HSM) is a physical computing device that protects and manages private keys and seed phrases, performs encryption and decryption functions for digital signatures, authentication, and other cryptographic functions. Hardware security modules can be used for the secure generation of digital asset keys. DDs providing digital asset custody services may use HSMs in order to securely store private keys or seeds in cold storage. For additional information on cyber security risks see the *DD Information Security Examination Manual*.

DDs may operationalize HSMs in a number of different ways. For example, DDs could send an encrypted message, from an external wallet application, to the HSM to sign the transaction. DDs could also extract a private key / seed stored in the HSM and then use the private key / seed to sign a transaction or deploy business logic into the HSM itself (which may create additional channels for attack vectors from executing code streams). Irrespective of how HSMs are deployed, the access control mechanisms and workflows for the communication with HSM must be highly secure.

Trusted Execution Environment

DDs may utilize a trusted execution environment ("TEE") to store private keys and sign transactions. Trusted execution environments are secure areas within processors that provide security features such as isolated execution, integrity and confidentiality to the data and programs running within it. The use of a TEE may provide DDs with the ability to store private keys and sign transactions with a greater level of security than is possible with a standard operating system. DDs that utilize TEE should ensure that their access control mechanisms and workflows for communication with TEEs are highly secure.

Single Private Key / Seed Phrase Signature Scheme

A single private key / seed phrase signature scheme refers to a method of signing transactions where only a single private key or seed phrase (e.g., Bip32 seed phrase) is required to create a signature and sign a transaction. Managing a single private key or seed phrase may offer less operational complexity compared to signing schemas that require multiple private keys or key shares; however, the use of a single private key or seed phrase may potentially represent a single point of failure and, if compromised, could result in the loss of the assets associated with its respective wallet address.

Transaction Signing via Multi-Signature Digital Asset Wallets

"Multisig" is a feature available on some distributed ledgers/blockchains that allow for multi-party authorization of a transaction, usually stylized as "M of N" where M is the threshold required for authorization, and N is the total size of the group. When setting up a multisig arrangement, a number of parameters can be chosen, such as whether the private keys are online, offline, or a mix of both and how they are stored and accessed; whether the multisig arrangement requires all keys to authorize a transaction, or whether a quorum smaller than the total group size is allowed to authorize a transaction. Multisig is often a native feature of a distributed ledger/blockchain, but there are some blockchains that do not natively offer multisig, hence users turn to multisig smart

contracts instead. Regardless of whether a native solution is used, security audits should look carefully at the implementation details chosen by a DD. Multi-sig digital asset wallets can be used to reduce digital asset custody risk by requiring multiple approvals before a transaction is executed. Using a multi-sig wallet, a digital asset custodian could implement internal controls such as requiring a quorum of signatories from different internal departments in order to sign a transaction thus mitigating the risk of internal theft. Thus, a multi-signature signing scheme can be used for authorization and audit purposes.

Multi-signature wallets can be configured on or off chain. Not all digital assets' underlying blockchains support multi-signature wallets and have signing protocols that require a single private key in order to execute a transaction. Protocols that do not natively support multi-signature wallets require off-chain encryption to implement a multi-signature signing solution. Off-chain multi-signature solutions work by encrypting the private key/seed using a multi-signature encryption. In this implementation, M of N signatures are required to access the private key/seed necessary to sign (execute) a digital asset transaction. Additionally, it may be possible to configure a multi-signature scheme (on a blockchain that does not inherently support multi-signature signing) through the use of a smart contract depending on the blockchain protocol.

Key Generation and Signing via Shamir's Secret Sharing Scheme (SSSS)

The Shamir's Secret Sharing Scheme (SSSS) is a cryptographic algorithm that enables the separation of a single private key into shards (the secret shares) so that each shard can be stored in different locations or be assigned to different parties. Similar to a multi-signature signing scheme, SSSS can enable M of N combinations of key shards to generate a single private key. In SSSS the key shards are used to generate the private key which is then used to sign a transaction. Therefore, SSSS may be vulnerable to external or internal theft when the private key is generated since the single private key can be used to sign transactions and may constitute a single point of failure. DDs that use Shamir's Secret Sharing Scheme should demonstrate that each private key shard associated with customers' digital assets is managed to the same level of compliance related to safekeeping, recording and transaction handling as a typical private key / seed phrase.

Key Generation and Signing via Multi-Party Computation (MPC)

Multi-party computation (MPC) is a general cryptography computation method that can be applied to many forms of computation, including multi-party transaction authorization, or signing. This is a protocol performed "off-chain," that is, it is not a system enforced by a blockchain but rather by other software and systems networked together for some purpose such as computing a transaction authorization. MPC is not widely standardized at this time, and each solution or use of MPC could refer to different protocols or systems that achieve different goals. For example, Shamir secret sharing can be considered a form of MPC, which is not equivalent to transaction authorization MPC protocols. Examiners should be careful to note what exact form of MPC or which algorithm is being used, and whether this algorithm and its implementation used by a DD has been examined by an appropriate auditor with expertise in advanced cryptography research.

Operational Considerations for Key Management

Given the unique risks associated with key management, DDs should implement strong operational controls to safeguard private keys and seeds, and the transaction signing process. Specific digital asset custody best practices and recommendations for key management/seed safekeeping are discussed below. DDs should ensure that information technology operational safeguards are subject to industry best practices to ensure a secure and stable custody operating environment. The operational controls implemented by DDs should be one element of an overall key management strategy, and supplement strong hardware and software solutions. Moreover, DDs may deploy risk mitigation tools in order to automate core digital asset custody functions such as transaction signing. In circumstances where DDs utilize tools to automate core functions, the tools deployed by the DD need to have received and passed a demonstrated risk assessment performed by a qualified third party. Corresponding operational risk procedures shall be documented. The DD shall implement risk monitoring mechanisms to identify failures in automation if they occur.

Secure Private Key and Seed Phrase Storage

To reduce the risks posed by third party cyber-attacks, DDs should implement policies, procedures, and programs to secure private key and seed storage to make it more difficult for malicious third parties to access and use custodied private keys or seeds through cyber-attacks or other means. DDs should have systems that provide periodic backups and operational redundancy to avoid single points of failure.

Key Management Storage and Signing Procedures and Protocols

Given the criticality of the key and seed management process to the safekeeping and custody of digital assets, the entire key management strategy should be described in functional documentation and subject to documented change approval processes. This should include the software and hardware security solutions employed, operational controls employed, the process used to securely sign and transmit transactions, and the flow of data between online and offline systems. Physical and system access by individuals is a critical operational control and should be carefully monitored and managed and documented in an auditable manner. Responsibility for manually executed (non-automated) core functions of custodial services should be performed by employees who have been subject to appropriate background screenings. DDs should review their private key and seed management strategy as part of their recurring operational risk assessment process. For additional discussion see the *DD Information Security Examination Manual.*

Designated Roles and Segregation of Duties

A DD shall have established roles and responsibilities for custodial service operations and custody operational risk management. To mitigate risks posed by insiders, DDs should require multi-signature arrangements to authorize transactions and otherwise carefully consider when segregation of duties is appropriate to mitigate the risks posed by a single insider. Separation of signing duties should prevent a linear ability to create, approve, sign transactions and broadcast to distributed ledger networks. A DD should require signoff of transaction from multiple individuals in different operational roles in order to reduce the risk of a quorum of individuals from acting in

bad faith to collude or manipulate automated systems. DDs should also use a system in which customer instructions for transactions may be authenticated or verified as genuine, and subsequently audited, to reduce the risk of theft and collusion. The use of automated systems may further reduce the risk of theft and collusion by eliminating the attack vectors associated with manual transaction signing. DDs should require each signatory to record their reasoning or evidence for the decision to authorize or reject the transaction.

A DD may also consider implementing increasing levels of security depending on the size and nature of a transaction. Each signatory should be able to be perform their duties independently of the others, and these processes should themselves be subject to user authorization and authentication controls to validate the signer's identity. DDs may also consider rotating the required signatories, transaction times and signing locations of custody transactions. Each signatory shall record their reasoning or evidence for the decision to authorize or reject each transaction. This evidence shall be retained and available for review. A DD may operationalize the segregation of duties through methods such as on or off-chain multi-signature schemes, multi- party computation, or through a workflow configured through their key management solutions or through some combination of these techniques.

Private Key / Seed Access Management and Revocations

Strict access management safeguards shall be in place to manage access to keys. DDs may put strict access management safeguards in place by implementing multi-factor authentication through methods such as the use of security badges, login credentials, tangible hardware, security tokens, and biometric data. Upon departure of a DD employee who had access to a digital asset wallet or knowledge of private key / seeds (including private key / seeds in a multi-signature or private key material in an MPC signature scheme) the DD should conduct an assessment to determine whether a new key ceremony and accompanying migration of digital assets is required. An audit trail shall record every change of access including who performed the change. Additionally, DDs should adopt procedures for the immediate revocation of a signatory's access. Key generation shall be performed in a manner in which a revoked signatory does not have access to the backup seed or knowledge of the phrase used in the creation. All keys shall be encrypted in a manner preventing a compromised signatory from recovering the seed. Procedures shall follow the standard protocol around removing user access without the need to create a new wallet.

Transaction Reconciliation and Auditability

DDs should maintain a full audit trail of all transaction activities. DDs' transaction records should include information such as the date and time of a transaction, transaction event type, jurisdiction of the customer, relevant signatories and the account balances and value of the transaction. Additionally, DDs should consider maintaining an auditable record (or "chain of custody") of all individuals who have or have had access to the private keys, backups, and hardware, as well as records of the specific individuals who participated in a specific withdrawal. Lastly, DDs should conduct ongoing monitoring and audit their transaction execution procedures to ensure that the necessary approvals occur, are recorded and that the transaction approvals are consistent with the transaction details recorded on-chain.

Employee Screening and Training

Due to the operational and internal theft risks posed to DDs engaging in digital asset custody, DDs should screen all employees appropriately and ensure adequate training and supervision at all times. DDs should provide industry-leading information technology security training on a regular basis to all employees and monitor their employee's compliance with established procedures. This training shall include potential attacks that are specifically applicable to digital assets.

Access to Secure Facilities and Monitoring

DDs should ensure they have physical access controls in place to prevent unauthorized internal or external access to their secure facilities. These controls should restrict access to secure facilities to individuals who require access for legitimate business needs. Records of each access attempt should be maintained. The list of authorized individuals should be continuously monitored and updated to reflect departures or role changes. Access policies should also consider dual controls and segregation of duties to mitigate risks from sole actors or staff collusion to the extent possible. DDs should consider supplementing access policies and controls with other physical security measures such as security cameras which are hardened against external attack. For additional information see the *DD Information Security Examination Manual*.

Business Continuity and Recovery

DDs should consider possible business continuity disruptions such as disaster scenarios and develop appropriate prevention and recovery plans. These plans should be documented, periodically reviewed, and updated. DDs should have a backup and redundancy plan for their custodied private key/seeds to avoid single points of failure. For example, a DD may choose to store HSMs across a number of secure locations. An alternative location used for private key and seed phrase storage should have appropriate distance between it and the primary custody location to mitigate environmental and technical interruptions at both sites. Additionally, DDs can use techniques such as multisig to store private key shares in multiple locations (in hot, cold or nearline storage) that must be brought together in order to sign a digital asset transaction.

9.8. Non-Custodial Key Management Services

A DD may facilitate through a third party, but not directly engage in, non-custodial key management services for multi-signature arrangements. Third parties that provide non-custodial key management services are not considered to have custody or control of an asset. An example of a non-custodial key management service is providing one of the required signatures in an M of N multi-signature scheme where the customer and their family member collectively hold a majority of the keys and the third party holds one key as a backup service.

While the risks associated with non-custodial key management services are reduced since the third party does not have complete control of the digital assets, third parties still face the same key management risks associated with custodial key management including (see *9.2 Private Key/Seed Management Risk Factors* section for additional information):

- Operational failure.
- Unauthorized access and use of private keys or seeds.
- Inaccurate record keeping and manipulation of logs/audit files

DDs should ensure that their third parties offering non-custodial key management services implement the same level of operational controls to safeguard the associated private keys and seeds during both the storage and transaction signing processes as with custodial key management services. See 9.6 *Private Key/Seed Management Risk Mitigation* section for additional information.

9.9. Source Code Version and Forking

Digital assets are underpinned by distributed ledger technology often in the form of blockchains. Blockchains rely on groups of decentralized computers or nodes working together to secure the network. The individuals or entities that operate nodes are referred to as "node operators". In order for nodes to access and secure the network, each node must run the same blockchain software. In a blockchain network, "forking" is essentially an update or change to the software that is collectively run by the nodes.

Soft Forks, Hard Forks, and Airdrops

Updates to blockchain software source code can occur via soft or hard forks. "Soft forks" are changes to the blockchain software that do not render the updated software incompatible with previous versions. In a blockchain network that has undergone a soft fork, the nodes running the updated software can still interact with nodes running previous versions of the software. A "hard fork" describes where the updates to the blockchain network render the new version of the blockchain software incompatible with the previous version of the software. A hard fork, "occurs when a cryptocurrency on a distributed ledger undergoes a protocol change resulting in a permanent diversion from the legacy or existing distributed ledger. A hard fork may result in the creation of a new cryptocurrency on a new distributed ledger in addition to the legacy cryptocurrency on the legacy distributed ledger."[63] Typically, hard forks are a result of material changes or updates to the underlying code such as changes in block size or consensus protocol (e.g., a change from proof of work to proof of stake).

When a blockchain network undergoes a hard fork, if a significant portion of the nodes do not adopt the changes to the blockchain software, the hard fork can result in the creation of two separate blockchains with a shared history. In this circumstance, the blockchain is bifurcated with nodes running the legacy software unable to interact with the nodes running the updated software. This is often referred to as a "contentious hard fork." In contentious hard forks that result in the bifurcation of a blockchain into two separate networks, owners of the native digital asset on the original network will (in addition to retaining ownership on the original blockchain) often receive a proportional amount of the new digital asset on the newly established blockchain. This is often referred to as an "airdrop." "A hard fork followed by an airdrop results in the distribution of units of the new cryptocurrency to addresses containing the legacy cryptocurrency."[64] Contentious hard

[63] 26 CFR 1.61-1: Gross income. (2019)
[64] 26 CFR 1.61-1: Gross income. (2019)

forks typically occur in open unpermissioned blockchain networks, such as the bitcoin or ethereum blockchains, rather than on permissioned blockchain networks where there is often some form of centralized governance among the node operators to drive blockchain source code updates.

Note: Airdrops do not only occur as a result of contentious hard forks. Airdrops are sometimes used as a marketing strategy for digital assets. Airdrops may select wallet addresses at random or through some other means to promote a new digital asset.

9.10. Source Code Version Updates and Forking Risks

DDs face a number of risks associated with source code version updates and blockchain forks; these risks are particularly pronounced when a hard fork has occurred establishing a new blockchain and is followed by an airdrop of new digital assets. Listed below are some of the risks associated with source code version changes.

Network Consensus and Signing Protocol Changes

Source code updates (e.g., a hard fork) may include significant changes to a blockchain's consensus mechanisms and signing protocols. These changes may present challenges to DDs providing digital asset custody services since they may render previously used software and hardware incompatible with the newly established network protocol, or in certain cases, allow malware access to private keys.

Network Bifurcation and Competing Blockchain Networks

A contentious hard fork may result in the creation of two separate digital assets supported by two independent blockchains. In a hard fork, the owner of the original digital asset may be rewarded a proportional amount of the new digital asset through an airdrop. Blockchain bifurcation that results in two competing digital assets may dilute the value of both digital assets similar to a stock split. Digital asset custodians should conduct a thorough evaluation and may need to update their policies, programs, and procedures in order to support the new digital asset in addition to the original digital asset.

Smart Contract Compatibility

Third parties that utilize smart contracts to issue tokens or provide services face the risk of their smart contracts becoming incompatible when blockchain source code updates occur. This risk is heightened in circumstances when a hard fork consisting of substantial protocol changes occurs. Third parties that utilize smart contracts may be required to create and deploy new smart contracts to support their products/services; the newly deployed smart contracts will need to be compatible with the most recent and widely supported blockchain source code version. This may require third parties to issue new tokens via an airdrop to replace previously issued (and now incompatible) tokens.

9.11. Risk Mitigation of Source Code Version Changes

DDs should develop strategies to identify, assess, monitor, and manage the operational risks posed by blockchain source code version changes. DD examiners should assess the policies, programs, and procedures DDs have in place to mitigate the risks associated with blockchain source code updates. Listed below are some of the source code version principles DDs should consider implementing to mitigate risks associated with source code version changes and protect their customers' assets.

Source Code Version Due Diligence

DD examiners should assess the due diligence conducted by the DD to anticipate any potential or upcoming blockchain source code version changes for each digital asset's underlying blockchain for which the DD provides custody services for. Source code changes may lead to, circumstances where is not possible to predict in advance whether utilization of the different source code version will be in the best interest of the customer. Additionally, the nature of proposed changes to source code versions from time to time may require the DD to consider the potential effects resulting from third-party actors (a person not a party to the agreement between the DD and its customer), who may create different source code versions resulting in new networks that could create economic value for the customers of the DD.

In circumstances where it is not possible to predict which source code version will be in the best interest of their customers, DDs should conduct sufficient due diligence to ensure they do not capriciously redefine the digital assets under their custody. DDs should consider assessing the nature of the source code version changes including but not limited to the reason for the updates, the blockchain protocol changes, whether a soft or hard fork will occur, the nodes supporting the updates, and whether a new digital asset will be created and an airdrop will occur.

In addition to conducting due diligence to determine which version of the blockchain source code software they will support, DDs should assess potential or upcoming blockchain source code changes with respect to their operations. Examiners should assess the controls DDs have in place to anticipate and mitigate the risk of source code version changes on their operations.

Key Management and Record Keeping for Airdrops

DD examiners should assess the policies, programs, and procedures DDs have in place to support key management and recordkeeping for digital assets acquired via an airdrop. Digital assets acquired through airdrops may utilize unique blockchain protocols and specific key management hardware and software requirements. For example, a hard fork may result in the creation of a new digital asset with a different signing mechanism when compared to the parent digital asset from which it was derived. The new signing mechanism might be insecure and might be able to leak information about the private key (such as the private key itself). For this reason, it should be considered insecure to use new untested software with private keys especially in a hard-fork situation. In this situation it is possible that a DD's hardware and/or software key management solutions (such as HSMs) used to facilitate digital asset transactions could be incompatible with the new blockchain protocol.

DDs should ensure their key management hardware, software and processes are compatible with assets acquired through airdrops (See section Operational Considerations for Key Management).

9.12. Proof-of-Work Digital Assets and Staking

Many digital assets (e.g., Tezos [XTZ], Cosmos [Atom], Dash [DASH], and Stellar [XLM]) utilize a blockchain network with a "proof of stake" consensus mechanism to validate transactions. These are often referred to as "proof of stake digital assets." In a "proof of stake" blockchain, network participants (or "nodes") can lock (or "stake") the network's native asset in a digital asset wallet in order to be eligible to validate the next block and earn "staking rewards." "Staking rewards" are a form of payment from the network in exchange for helping to secure the blockchain.

DDs may "facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to…staking".[65] "Proof of stake" digital assets typically have block validation rules with a pseudo-random election process to select a node to be the validator [66] of the next block. The block validation rules can be based on a combination of factors which may vary based on the blockchain network's source code version; examples include the staking age of the node (i.e., the length of time the node has been staking on the network), randomization, and the node's volume of digital assets under possession. Typically, the size of the stake (i.e., the number of native assets staked by the validator node) is directly proportional to that node's probability of being selected as the validator of the next block.

Depending on the blockchain protocol, the validating node's staking reward can be in the form of a newly minted digital asset or a transaction fee from the block that was added (or "forged"). There are no guaranteed returns for staking since there are no established orders for how staking rewards are distributed.

Criteria for Staking

To earn staking rewards, owners of proof of stake digital assets must place their digital assets in a suitable wallet and validate transactions in a manner that is consistent with the blockchain's protocol. Staked digital assets typically cannot be spent while they are staked on the network. Staked digital assets will often need to be held in a digital asset wallet that is connected to the internet or "hot wallet" depending on the consensus mechanism utilized by the blockchain. In addition to holding staked digital assets in a suitable wallet, proof of stake protocols typically has additional requirements such as minimum digital asset thresholds for staked assets and minimum durations digital assets must be staked before they are eligible to earn staking rewards.

Staking Services

Staking requirements and the technical complexity of staking often makes staking infeasible for investors. Staking services may also offer benefits to investors such as additional flexibility to withdraw funds and more secure safekeeping of assets. DDs may facilitate (but not directly

[65] Neb. Rev. Stat. § 8-3005(2)(b) (LB707, 2022)
[66] The validator node is responsible for verifying transactions within a blockchain.

provide) staking services to their customers as a way for customers to generate passive income on their digital assets similar to earning interest in a traditional savings account. Staking services typically charge a fee as a proportion of the rewards. Rewards earned through staking service providers are re-distributed to investors with the staking service provider usually taking a percentage of the attributed block rewards as a fee.

Staking services pool staked digital assets (known as "staking pools") from many investors (ensuring digital asset threshold and duration requirements are met) and handle the technical aspects of staking; thus, removing many of the barriers to staking for investors. Depending on the underlying blockchain's protocol, staking pools may require the aggregation of staked assets into a single shared digital asset wallet controlled by the staking service provider. Other blockchain designs (such as delegated proof of stake blockchain designs (or "DPoS")) permit the delegation of staked assets; this enables staked digital assets to be held offline (or in a "cold wallet") and delegated to a validator node.

9.13. Staking Service Risks

Unauthorized Access to Staked Digital Assets

Third parties providing staking services for customers face the same risks of unauthorized access to private keys or seeds as typical digital asset custodians who do not provide staking services. However, certain proof of stake protocols may require digital assets to be pooled together in an omnibus account. Additionally, dependent on the digital asset's underlying blockchain, staked assets may be required to be held in a hot wallet. These staking pools heighten the risks associated with unauthorized access since these "honey pots" become attractive targets for internal and external malicious actors who may attempt to obtain control of the associated private keys or seeds.

Slashing or Forfeiture of Funds

Many proof of stake protocols have mechanisms in place (in the form of penalties) to disincentivize abnormal or malicious behavior that is detrimental to the blockchain network. These mechanisms are often referred to as "slashing" penalties. "Slashing" is a penalty imposed on the validator node by the blockchain network if the node attempts to validate transactions in a manner that is inconsistent with the blockchain's protocol (often referred to as "consensus fault slashing") or if the node fails to provide reliable uptime in support of the network (often referred to as "storage fault slashing"). For example, a consensus fault slashing penalty could be imposed on a validator node if the node attempted to double-sign a transaction in error. Examples of storage fault slashing could include slashing penalties imposed on a validator node that is unexpectedly taken offline (and therefore not supporting the network) for a period of time. Critically, slashing penalties will vary dependent on the underlying protocol of the staked digital assets.

"Slashing" typically results in a forfeiture of funds by the responsible validator node. Third parties providing staking services and their customers could face slashing penalties if they intentionally or unintentionally make an error (commit a fault) when conducting their staking responsibilities (i.e., validating transactions) on the network.

9.14. Responsibilities of a DD for Facilitated Staking Service Activities

Examiners should determine whether DDs facilitating staking through third parties ensure that those third parties have adequate systems in place to identify, measure, monitor and manage risks associated with staking services. Third parties should have policies, programs, and procedures to mitigate the risks associated with providing staking services.

An example of such controls may include substituting the third party's assets in lieu of customer assets in a staking arrangement. In this model customers may engage in staking; however, the third party provides their own digital assets to be stored online as a proxy for their customers' assets whose "staked" assets remain in cold storage or some other equally secure key management solution. This enables customers to earn a portion of the staking rewards while mitigating the risks posed by slashing and by unauthorized access through cyberattack.

Additionally, DDs should ensure that third parties conduct appropriate source code due diligence to ensure the source code version of the blockchain software run by their nodes is current and capable of performing staking operations consistent with the blockchain protocol (S*ee section 9.11 Risk Mitigation of Source Code Version Changes*).

9.15. Customer Protections, Agreements and Notifications

DDs that provide custody services are expected to enter into a written custody agreement with their custody clients clearly setting forth the roles and responsibilities of the custodian and customer, the terms and conditions of the custodial relationship, and what authorities the client wishes for the custodian to exercise over the assets. The responsibilities for the DD include obtaining customer agreements, implementing appropriate controls to protect customer's custodied assets and providing notifications to customers when necessary.

Agreements & Notifications for Digital Asset's Source Code Version

Changes to the blockchain source code version can have a significant impact on the value and nature of digital assets as well as on a DD's operations. [67] DDs must implement policies, programs, and procedures to support customer protection, agreements and notifications related to source code version support and changes.

A DD and its customer shall agree in writing regarding the source code version the DD will use for each digital asset. In circumstances where the agreed upon blockchain source code undergoes a hard or soft fork a DD may periodically determine whether to implement a source code version that uses block validation rules different than those of the source code version specified in the customer agreement. This includes circumstances where it is not possible to predict in advance whether utilization of the different source code version will be in the best interest of the customer. In situations where the blockchain source code change is likely to have a material impact on the economic value of the customer's digital assets, DDs shall have a duty to provide higher standards

[67] See *9.9 Source Code Version and Forking* section for additional information

of customer notice and acknowledgement of the blockchain source code changes and their potential and actual effects on custodied digital assets.

The following are scenarios where DDs are required to obtain customer agreements for, and provide notifications and acknowledgements of, blockchain source code changes. Accordingly, examiners should assess the DD's systems, documentation, and processes and identify potential gaps:

1) In circumstances where the DD chooses not to continue to support the original source code version agreed upon with the customer, the DD will be required to obtain affirmative consent from the customer if the following conditions occur:

    a) The DD seeks to implement a source code version that uses a consensus rule that differs from the original, as defined by the source code version specified in the customer agreement;

    b) The DD will not continue support for the original source code; and

    c) The original source code version continues to exist or is reasonably expected to continue to exist.

2) In circumstances where the DD continues to support the original source code version agreed upon with the customer and implements a new source code version that uses a consensus rule that differs from the original, the DD must make reasonable efforts to notify their customers if any of the following conditions occur:

    a) The DD determines to implement a new source code version that uses a consensus rule that differs from the original that is specified in the customer agreement;

    b) The DD will continue to support the original source code version specified in the customer agreement; and

    c) The original source code version continues to exist or is reasonably expected to continue to exist.

3) In circumstances where the original source code version no longer exists, or is not reasonably expected to continue to exist, the DD must make reasonable efforts to inform their customers of the source code changes from the original agreed upon source code version if all of the following conditions occur:

    a) The DD determines to implement a new source code version that uses a consensus rule that differs from the original that is specified in the customer agreement;

    b) The DD will no longer accommodate the source code version specified in the customer agreement; and

4) The original source code version no longer exists or is not reasonably expected to continue to exist. In all other circumstances, the DD shall make reasonable efforts to notify the customer

regarding source code version changes and act in a manner that the DD reasonably believes will be of economic benefit to the customer.

The notice requirements for source code version changes are not applicable to security vulnerabilities or other emergencies, as reasonably determined by the DD. After a source code version change relating to a security vulnerability or other emergency which would affect block validation rules, the DD shall provide written notice of the change to each customer as soon as practicable to minimize the security risk to customer assets. In case a DD's customers have not maintained current contact information, DDs will be deemed to have met notice requirements if it provides notice through its website and other media routinely used by the DD.

Customer Protections, Agreements & Notifications for Digital Asset Custody Services

In addition to obtaining customer agreements and providing notifications for source code version changes, and in addition to custody agreement requirements specified in *Chapter 7.3* of this Manual, DDs must provide clear notice to their customers of the following. Accordingly, Department examiners should assess the DD's systems, documentation, and processes and identify related gaps:

- The heightened risk of loss from transactions facilitated through third parties, such as the buying and selling of digital assets, participating in staking services, derivatives, exchanges of fiat and virtual currency (on/off ramps), digital asset lending, and other classes of facilitated transactions approved by the Director in writing in advance of the transaction.

- For a third party's asset pooling arrangements, including proof-of stake digital assets, masternodes or similar arrangements, a DD shall additionally provide a description of the security measures the third party will undertake to manage risk of loss. For additional information on security measures that third parties may take for asset pooling arrangements see Responsibilities of a DD for Facilitated Staking Service Activities.

- That there is some risk of loss as a pro rata creditor due to custody of a fungible asset or custody under a bailment where the DD may undertake transactions with a digital asset on the customers behalf.

- That custody under a bailment may not result in the digital assets of the customer being strictly segregated from other customer assets. For more information refer to Digital Asset Custody Models [Omnibus versus Segregated Accounts].

- That the DD is not liable for losses suffered as the result of transactions facilitated through third parties (such as the buying and selling of digital assets, participating in staking services, derivatives, exchanges of fiat and virtual currency (on/off ramps), and digital asset lending except for liability consistent with the DD's fiduciary and trust powers as a custodian under this section.

- That a DD and its customer shall agree in writing to a time period within which the DD must return a digital asset held in custody.

- If the DD may, based on customer instructions, undertake transactions with a digital asset then the DD and the customer may also agree in writing to the form in which the digital asset shall be returned.

- That all ancillary or subsidiary proceeds relating to digital assets held in custody, commonly known as forks, airdrops, staking gains or similar proceeds from offshoots, including interest, shall accrue to the benefit of the customer, except as specified by a written agreement with the customer. The DD may elect not to collect certain ancillary or subsidiary proceeds, as long as the election is disclosed in writing.

    - That a DD shall enter into a written agreement with a customer, if desired by the customer, regarding the manner in which to invest ancillary or subsidiary proceeds or other gains attributable to digital assets held in custody.

    - That a DD shall not authorize or permit rehypothecation of digital assets under its custody. The DD shall not engage in any activity to use or exercise discretionary authority relating to a digital asset except based on customer instructions.

    - That in order to promote legal certainty and greater predictability of digital asset transactions, a DD and a customer may define in writing the terms of settlement finality for all transactions.

        - Agreements between the DD and the customer must address:

            a) The conditions under which a digital asset may be deemed fully transferred.

            b) The exact moment of transfer of a digital asset.

            c) The discharge of any obligations upon transfer of a digital asset.

9.16. Examination Procedures

Procedure	Comments
Digital Asset Safekeeping A DD is responsible for maintaining the safety of custodied digital assets held in digital form at one of the custodian's premises, a sub-custodian facility, or an outside depository. Objective: Given the size and complexity of the DD, determine whether DD management and personnel display acceptable knowledge and technical skills to ensure proper safekeeping of digital assets.	
1. Evaluate the adequacy of audit and control processes related to on-premises and off-premises safekeeping. Consider: • The scope of the audit coverage. • The size and nature (age) of exceptions reported. • Charge-offs due to lost or stolen securities.	
2. Using what you have learned from performing these procedures, evaluate the knowledge, communications, and technical skills of management and staff members.	
Private Key and Seed Management Due to the nature of digital assets, DDs must provide safekeeping for all of the private keys associated with the addresses where their customers' digital assets are held and maintain exclusive control or possession over these keys. Objective: To determine the effectiveness of the control processes for private key / seed management associated with customers' custodied assets.	
1. For digital asset custody activities, determine whether appropriate policies, procedures and programs have been implemented to assure safekeeping of custodied digital assets. Consider: • Mechanisms the DD has in place to assess its liquidity needs • Whether the private keys associated with the majority of assets under custody not required for customer transactions are held in cold storage. • Whether the DD only maintains private keys required for customer transactions in hot storage. • The DD's internal controls and audit	

Procedure	Comments
procedures relating to its mechanisms and thresholds in place to facilitate the transfer of assets between different storage methods (such as hot and cold storage). • The DD's ability to perform permissible transactions in a timely manner to provide liquidity to customers. • The DD's ability to obtain insurance or other forms of risk mitigation and how these considerations inform its private key storage policy. • The DD's ability to manage the same level of compliance related to safekeeping, recording and transaction handling for each digital asset it provides custody services for. • Whether the DD generates seeds using National Institute of Standards and Technology (NIST) compliant deterministic random bit generator, secure non-deterministic key generation mechanism, or other method approved by the Director. • The DD's use of omnibus and segregated accounts and whether appropriate key management and record keeping policies, programs and procedures have been implemented for each model used by the DD. • Each technique used by the DD to ensure secure storage of private keys and seeds in order to limit access to approved individuals. • The technology used to support key management operations including HSMs, secure enclaves, multi-signature wallets, MPC, etc. • The DD's controls and procedures for the audit and maintenance of physical storage devices to prevent hardware failure. • The DD's procedures for testing and auditing of digital asset signing	

Procedure	Comments
procedures to prevent vulnerabilities from cyberattack. • Whether the DD has designated roles and a separation of duties for signing digital asset transactions. • Controls the DD has implemented to prevent unauthorized access and use of private keys/seeds from internal malicious actors • Whether the DD maintains accurate records and logs for digital asset transactions including signatories, private keys used, time, date, digital asset type, amount, etc. • Whether the DD has controls in place to confirm the validity of all digital asset transactions executed using private keys. • Whether employees who are responsible for custodial duties have been subject to appropriate background screenings. • The DD's physical access controls in place to prevent unauthorized internal or external access to their secure facilities. • Whether the DD has documented plans for business continuity disruptions such as disasters scenarios and has developed appropriate prevention and recovery plans. • If the DD has deployed risk mitigation tools to automate certain core functions, consider whether these tools have passed a demonstrated risk assessment performed by a qualified third-party. • Controls the DD has implemented to mitigate the risks associated with the safekeeping of digital asset storage devices such as HSMs.	
Source Code Version and Forking	

Procedure	Comments
DDs face a number of risks associated with source code version updates and blockchain forks and must have policies, programs, and procedures to address these risks. Objective: To determine the effectiveness of the policies, programs, and procedures the DD has implemented in order to address risks posed to custodied digital assets by blockchain source code version changes such as hard and soft forks and airdrops.	
1. Evaluate the DD's policies, programs, and procedures to mitigate the risks associated with blockchain source code updates. For each digital asset supported by the DD, consider: • DD's processes to anticipate source code version changes to a supported digital asset blockchain's source code version • DD's procedures for due diligence of upcoming source code version changes and the potential effects of the source code changes on their operations • DD's controls for ensuring that custodied assets are not capriciously redefined during source code version changes	
2. For "airdrops", determine whether DDs have sufficient processes in place to support the new digital asset. Consider: • The DD's controls for ensuring accurate recordkeeping when an "airdrop" has occurred • The DD's key management procedures with respect to "airdrops" to ensure that digital assets acquired through "airdrops" are compatible with key management hardware and software solutions	
Proof-of-Work Digital Assets and Staking In addition to typical key management controls DDs should ensure that third parties which are used to facilitate staking activities implement policies, programs, and procedures to mitigate the risks associated with providing staking services. Objective: DD examiners should determine whether DDs facilitating staking services through third parties ensure that third parties have adequate systems in place to identify, measure, monitor and manage risks associated with staking services.	

Procedure	Comments
1. For each digital asset that the DD facilitates staking of through a third party, determine whether the DD's third parties providing staking services have adequate systems in place to identify, measure, monitor and manage risks associated with staking services. Evaluate the DD's process to assess the following at third parties used to facilitate staking: • Controls for ensuring that internal or external malicious actors do not gain unauthorized access to staked digital assets. • Whether the private key(s) or seeds for customer's staked digital assets are held in a storage solution that is connected to the internet. • Whether customer's staked digital assets are held in omnibus staking accounts. • Controls in place to ensure that customer funds are not forfeited by "slashing" or similar protocols by the network.	
Customer Protections, Agreements & Notifications for Digital Asset Custody Services Changes to the blockchain source code version can have a significant impact on the value and nature of digital assets as well as on a DD's operations. DDs must implement policies, programs, and procedures to support customer protection, agreements and notifications related to source code version support and changes. Objective: To determine the effectiveness of the controls, policies, programs, and procedures to support customer protection, along with agreements and notifications related to source code version support and changes.	
1. Assess the DD's policies, programs, and procedures to support customer protection, agreements and notifications related to source code version support and changes. Consider: • Whether the DD has obtained written customer agreement regarding which source code version(s) they will use for each digital asset for which they provide custody services. • DD's procedures for notifying and	

Procedure	Comments
obtaining agreement for source code version changes for each digital asset for which they provide custody services for.	
2. Assess the DD's policies, programs, and procedures to support customer protection, agreements and notifications related to digital asset custody services. Consider: • The DD's procedures for providing clear notice of the heightened risk associated with digital asset activities facilitated through a third party such as buying/selling digital assets, staking, derivatives, etc. • Whether the DD provides clear notice to customers of the measures its third parties take to protect customers' staked digital assets from losses. • Whether the DD provides clear notice that risk of loss as a pro rata creditor exists due to custody of a fungible asset. • Whether the DD provides clear notice that custody under a bailment may not result in the digital assets of the customer being strictly segregated from other customer assets. • Whether the DD provides clear notice that the DD is not liable for losses suffered as the result of facilitated transactions except for liability consistent with the DD's fiduciary and trust powers as a custodian. • Whether the DD has obtained written agreement to a time period within which the DD must return a digital asset held in custody and (if applicable) the form the digital asset shall be returned. • Whether the DD provides clear notice that all ancillary or subsidiary proceeds relating to digital assets held in custody, commonly known as forks, airdrops, staking gains or similar proceeds from offshoots, including interest, shall accrue to the benefit of the customer, except as specified by a written agreement with the customer (and,	

Procedure	Comments
whether, in such cases, the DD has obtained the customer's written agreement). • Whether the DD provides clear notice that the DD shall not authorize or permit rehypothecation of digital assets under its custody. The DD shall not engage in any activity to use or exercise discretionary authority relating to a digital asset except based on customer instructions.	

10. ASSET LENDING

While digital asset lending has only emerged in recent years, securities lending has a long history dating back to the 1960's and has evolved into one of the most important value-added products traditional bank custodians offer to their customers. Bank custodians have traditionally acted as the lending agent for customers' securities lending activities; however, because the securities lending market is extremely competitive, third-party intermediaries have emerged. Wholesale intermediaries conduct transactions directly with the lender and the borrower, becoming a principal to the transaction. Niche intermediaries may specialize in particular types of securities loaned or aggressive cash collateral reinvestment programs. Third-party intermediaries may target clients that are dissatisfied with the performance of their custody banks. Internet auction systems for securities lending are being started up. These auctions, which bring lenders and borrowers together, may eliminate custodian and third-party intermediaries. The discussion in this section is limited to a custodian's role as lending agent for its customer and focuses on the novel issues presented by lending digital assets over traditional securities lending activities.

This section generally applies to securities lending operations, including for digital assets that may be securities. While the standards of this section should be viewed as a best practice for other digital asset lending transactions, the Department recognizes that some standards may not be applicable to commodities lending transactions, including for virtual currency. A DD should consult with the Director on the applicability of a particular standard to commodities lending so that the transaction may be appropriately structured consistent with safe and sound bank practices under federal and Nebraska law.

The Evolution of Securities Lending Markets

The securities lending markets have existed in the United States since the 1960s, when an active inter-dealer market developed. In the 1970s, U.S. custodian banks first began lending securities to brokers on behalf of their clients. Demand for securities lending increased as new forms of trading strategies emerged. In 1982, the collapse of a U.S. securities dealer led to a number of reforms, including standardized agreements and collateral margins. The 1980s also saw a dramatic increase in the size of government securities markets in the United States and many other countries. Growth of securities lending in some foreign markets was hampered by concerns about the legalities of transactions, unfavorable tax treatment, and assorted regulatory restrictions. This resulted in the development of "offshore" securities lending markets, where securities lending transactions were settled on the books of foreign sub-custodians. This offshore activity fed increasing demand for non-U.S. securities. In the 1990s as growth of securities lending continued, such lending expanded into emerging markets. In the wake of this growth, many foreign markets have worked to address legal, tax, and regulatory issues impeding securities lending activities.

The globalization of securities markets, the consolidation of financial intermediaries, and shortened settlement cycles will have a significant impact on how the industry continues to evolve. These industry developments are designed to lend efficiency and innovation to the market and will present a challenge for custodians maintaining a securities lending strategy.

The Role of Bank Custodians

Custodian banks have traditionally been the primary lending agent or intermediary, bringing borrowers and lenders together for a fee. Custodians require a large base of lendable assets to make their lending program profitable. Other portfolio-related factors that may affect the success of a bank's securities lending program are:

- Portfolio composition. If the portfolio is made up of assets widely available in the market, the demand for those assets may be low, making it difficult to locate a borrower. In contrast, a portfolio made up of assets in high demand will be easier and more profitable to lend.
- Portfolio management style. A portfolio that is actively managed is generally less attractive to borrowers than a passively managed portfolio because its turnover is likely to be higher. High turnover can lead to inconvenient recalls of loaned assets.

In addition to providing the lendable assets, custodians typically provide settlement services for the lending transaction, and safekeeping and/or investment management services for the collateral, which are discussed elsewhere in this Manual.

Finders

Finders are fully disclosed intermediaries who bring lenders and borrowers together. If the DD is a finder, it may receive either a finder's fee (flat fee) or a revenue-based fee. Some DDs may use a finder to attract securities lending customers. A DD using a finder should have written policies covering the circumstances in which a finder will be used, which party pays the fee (borrower or lender), and which finders the institution will use.

10.1. The Asset Lending Transaction

An asset lending transaction is essentially the temporary, collateralized loan of an asset by the owner (lender) to a borrower, for a fee. Asset lending adds liquidity and efficiency to the markets and supports trading activities and strategies in the United States as well as other major markets.

Parties to the Transaction

Lenders of securities and other assets are typically institutional investors with large investment portfolios such as investment funds, pension plans, insurance companies, and endowments. The primary borrowers of assets, at least in traditional markets, are typically broker-dealers or large investment funds, who typically borrow the asset to facilitate a short position in the asset.

Reasons Parties Engage in Asset Lending

Borrowers may engage in asset lending for a variety of reasons, including to cover short sales or failed trades, or to execute hedging or arbitrage strategies. Lenders engage in asset lending transactions as a means of increasing the incremental yield on their investment portfolios.

Transfer of Legal Title and Benefits

The legal title to the assets loaned passes to the borrower for the term of the loan. This may apply to digital assets as well, in the context of various commercial law, securities, commodities, and tax law requirements. Examiners should carefully note the structure used by a specific DD and the legal/supervisory reasons for doing so. The lender regains title when the assets are returned. In the case of a security, although the lender temporarily loses legal ownership, the economic benefit of any derived income payments connected with the asset on loan are retained through the use of "manufactured payments" from the borrower to the lender. However, the lender loses voting rights associated with the asset during the term of the loan, and the "manufactured payments" may be subject to alternate tax treatment compared to direct payments from holding the asset. The detailed legal rights and obligations of the parties to an asset lending transaction should be set out in written agreements. Refer to the *"Due Diligence Considerations"* section below for additional information.

In the case of a digital asset, events might also occur while the asset is lent to the borrower which require proactive action or management, such as forks or asset governance events. A DD is expected to have clearly described the rights and responsibilities of each party in a lending transaction in the terms and conditions and other written agreements governing a digital asset loan.

Collateral

The primary forms of collateral used for an asset lending transaction are cash, securities, or a standby letter of credit. If cash is provided as collateral, the lending agent or intermediary (e.g., the custody bank) will typically be responsible for investing the cash for the term of the loan. Providing cash collateral is the prevalent market practice in the United States. When securities are provided as collateral, the lender will typically specify the type of securities that are acceptable (e.g., government securities, minimum credit rating). Use of securities as collateral is common in most non-U.S. markets. Value of the collateral provided generally exceeds the value of the securities loaned. Collateral margins are discussed further in the *"Security Interest/Collateral Management"* section below.

The Department does not prohibit the pledging of other assets, including digital assets, as collateral. Lending arrangements collateralized with less traditional and potentially more volatile assets should be clearly agreed to by the parties to the transaction and contingencies related to the possible price movements in the price of collateral should be clearly articulated in the lending agreements. The Department also expects that a DD will take into account the nature of the collateral and the market for the collateral in establishing collateral requirements in a lending agreement.

A security interest, or other method typically used in commodities markets, may be appropriate instead of posting collateral, consistent with safe and sound banking practices.

Fees

The fee paid by the borrower will depend on the type of collateral for the loan. The fee may also vary with the supply and demand for the asset borrowed. If the collateral for the loan is a security

or a letter of credit, the borrower will pay a negotiated fee to the lender. If cash secures the loan, the borrower typically receives a negotiated rate of return (the rebate rate) on the collateral. The rebate rate is typically based on benchmark rates such as the Fed Funds rate, the Repo rate, or a LIBOR replacement. The lender is entitled to retain any income earned on the reinvestment of the cash collateral in excess of the rebate rate. Typically, the lender and the lending agent (custodian) split the excess income.

Manufactured Payments

Typically, in a securities lending transaction, the borrower agrees to make "manufactured payments" to the lender to replicate the economics of cash flows or other benefits that the lender would be entitled to if it had continued to hold the asset (e.g., equity dividends or fixed income coupon payments). Lending agreements for digital assets, when title to the assets passes to the borrower, should also include provisions to provide for the "manufacture" of benefits to a lender that it would be entitled to if it continued to hold the asset, if any.

In drafting lending agreements, a DD should carefully consider what, if any, benefits would need to be manufactured based on the design of each digital asset in its lending program. The Department does not expect that such manufactured payments would be expected for many of the most prevalent digital assets, at the time of this writing, such as bitcoin. Lenders of assets that may receive benefits from, for example, staking, may require manufactured payments. Alternatively, lenders may agree to transfer these benefits to the borrower. The Department does not have a view on how these lending transactions should be structured to account for these scenarios, but only that the lending agreements clearly articulate the terms to avoid confusion, disputes, and support risk management. Lending agreements should also provide for events outside the design of the asset, such as "forks" and "airdrops."

In the case of digital assets in which title does not pass to the borrower, the DD should generally specify in relevant agreements the method in which forks, airdrops, staking and other ancillary or subsidiary proceeds are allocated and managed.

10.2. The Digital Asset Lending Market

The digital asset lending market has developed over the past several years, led by non-bank entities that have, to some extent, modeled themselves on the practices of securities lenders in the more traditional financial markets. However, the digital asset lending markets are nascent and subject to regulatory and legal uncertainties (including whether lending is enforceable and the effectiveness of certain types of liens), in addition to being subject to other novel risks associated to the unique features of digital assets.

Currently digital asset lending markets are largely unregulated. See *11. CEA AND CFTC Compliance Considerations* section for a discussion of related regulatory considerations. Currently the market is dominated by custodians and digital asset exchanges that offer interest rates well in excess of what is offered by US banking institutions on custodied securities that customers make available for lending. These market participants rely on proprietary risk management methods, often backed by external insurance coverage.

In consideration of the elevated risks in this space, the Department has more restrictive practices and higher standards for risk management than what might be typically found in similar lending businesses by traditional securities custodians.

10.3. DD Specific Considerations

Custodial lending programs of digital assets by DDs will differ from the typical securities lending by bank custodians in at least the following four key ways:

- The specific digital assets that may be included in an asset lending program must be approved by the Department either as part of the initial charter application, or through subsequent consultation and approval.
- A DD may employ a security interest for certain virtual currency transactions instead of using collateral to secure the loan. The security interest may not be in an asset subject to a lending transaction, but rather may be another asset which serves a similar purpose as posting collateral.
- Lender-customers assume most risks of potential loss from participation in the lending program. Traditional bank custodians have offered indemnification from losses by borrowers in exchange for a fee as part of their lending programs. This should not be construed to mean that DDs cannot take reasonable and prudent steps to reduce or limit customer exposure to potential losses or to provide indemnification in certain scenarios. Additionally, DDs retain fiduciary and trust liability responsibility for the execution of a lending transaction.
- DDs are prohibited from rehypothecating pledged assets.

Each of these considerations will be discussed in further detail below.

10.4. Assets Subject to Facilitated Lending Programs

Applicants for a DD charter are expected to identify the specific digital assets they will offer custody services for as part of the business plan submitted during the application process, or as part of a subsequent request for approval. Moreover, the Department expects that a DD will tailor the suite of products and services offerings applicable to each digital asset based on an analysis of the risks and market for each digital asset.

The Department expects that the assets and facilitated service offerings of a DD should be calibrated to the profile and resources of an individual DD.

Once a DD is chartered, the Department expects DDs to continue to consult the Department and seek approval for any changes to the assets it will support with custody services. See *13. Digital Asset Due Diligence and Permissibility* section for more details.

Factors that a DD should consider when evaluating an asset for inclusion in a facilitated lending program include:

- Liquidity, trading volume, volatility, and turnover;
- Historical volatility;
- Distribution of asset holders;

- The administration and governance of the asset; and
- Asset-specific risk concerns (e.g., legal status, AML/KYC compliance, security, regulatory events).

Due Diligence Considerations

A DD should have board-approved facilitated asset lending policies (or policies approved by a designated committee) in place prior to engaging in facilitated asset lending activities. The DD should ensure that written agreements are in place with potential borrowers and with customers participating in the facilitated lending program. Due diligence reviews should be conducted on potential borrowers, and counterparty credit limits should be established.

Loan Agreement

The DD should ensure that written agreements are in place before facilitating an asset lending transaction with a borrower. In the securities markets, master agreements, which detail the duties and responsibilities of each party were initially developed to manage risks resulting from a broker failure. In the United States' securities markets, the most widely used securities lending agreement is the Master Securities Loan Agreement published by the Bond Market Association (formerly known as the Public Securities Association). The most widely used global master securities lending agreement is the Overseas Securities Lending Agreement. Banks in all G-10 countries use master agreements to establish terms and conditions, as well as to manage risk. Some banks use standard agreements developed in-house; others negotiate each agreement.

In the digital asset lending markets, some of the early entrants have developed master digital asset lending agreements modeled on those widely used in the securities markets.[68] While digital asset agreements should consider existing agreements in securities and commodities markets, the Department does not mandate any agreement format for digital asset lending. A DD should, however, strive to use the same agreement format for each of its customers. At a minimum, the written agreements with the borrower should address, when taken together, and as applicable:

- Transfer of legal title or security interest, structure of the transaction;
- Length of the loan;
- The risks assumed by the parties to the transaction;
- Acceptable forms of collateral, margin requirements or security interests;
- Valuation of collateral and margin calls (as applicable);
- Manufactured payments (as applicable);
- Rebate rates or other fees;
- Termination of the loan and a time for return of the asset;
- A pledge not to further hypothecate the asset;
- Treatment of liens;
- Applicable law; and
- Events of default.

[68] Lendingblock. "Global Digital Assets Lending Agreement" (July 30, 2019)

DDs should use master or standard agreements whenever possible. The DD's legal counsel should thoroughly review each master and standard agreement and all facilitated lending arrangements that do not use the DD's standard documents.

Agency Agreement

It is important that the DD have written agreements with all facilitated lending customers that clearly delineate the duties and responsibilities of the DD as the customer's lending agent. Note that agreements between the DD and its customers should not include any duties, responsibilities, or abilities which constitute more than mere "facilitation" of a lending transaction, and that they do not allow for the DD to engage in any activity which is not permitted by the NFIA. At a minimum, the agreements should, when taken together, address:

- Acceptable forms of collateral and margin requirements;
- Reinvestment of cash collateral;
- Fee schedule;
- Approval of borrowers;
- The risks assumed by the parties to the transaction, and the expressed lack of guarantee or indemnification by the DD;
- Termination of the loan and the time the asset will be returned;
- Manufactured payments or other subsidiary or ancillary value;
- Applicable fiduciary and trust liability of the DD for the transaction;
- Applicable disclosures required under Neb. Stat. § 8-3008.
- Events of default.

A customer may use the agreement to customize its asset lending program. For example, the customer can establish its own cash collateral investment guidelines or may limit acceptable borrowers to those with a minimum credit rating.

Selection of Borrowers

The risk arising from a borrower's default may be significant. The DD should have a well-developed, independent process in place to scrutinize borrowers. Once approved, borrowers should be reviewed periodically. Many bank custodians rely on bank credit departments to analyze the credit risk of their borrowers. Factors that should be considered by a DD during selection and ongoing review of a borrower include:

- Financial condition;
- Risk profile, including an evaluation of how the borrower typically uses borrowed assets;
- If applicable, IT framework and policies;
- AML/BSA/KYC and sanctions verification; and
- The borrower's overall reputation and history with the DD and other institutions.

The DD should establish a credit limit for each borrower. The limit should be based on the customer's total exposure to the borrower. In addition to an overall credit limit, a DD may consider setting specific limits for given digital assets based on other factors, such as market volatility and liquidity.

10.5. Digital Asset Lenders Must Assume Risks

As a term of participation in a DD's facilitated lending program or transaction, all risks of loss (other than fiduciary or trust liability for execution-type failures) must be assumed by the DD's customers. Lending agreements should indemnify the DD for liability in these transactions. In addition, DDs are prohibited from engaging in lending activities using customer deposits.

It is common for an institution offering traditional securities custody and security lending services to offer indemnification against borrower default in exchange for a fee. These arrangements are prohibited.

10.6. Laws and Taxation

The laws and taxation applicable to asset lending transactions may vary significantly from market to market.

Legal Constraints on Some Lenders

A customer's participation in an asset securities lending program may be affected by statutory or regulatory restrictions. The most common example is a U.S. pension account that is subject to ERISA.

The DOL allows qualified employee benefit plans subject to ERISA to participate in securities lending programs if certain conditions are met. Prohibited Transaction Exemption (PTE) 81-6 details those conditions. In general, the conditions required by the DOL conform to industry standards.

A bank may act as a lending agent and receive reasonable compensation from covered plans provided the loan of assets is not prohibited by section 406(a) of ERISA. PTE 82-63 authorizes the lending agent to engage in securities lending on behalf of a plan and receive reasonable compensation paid in accordance with a written agreement. However, an independent plan fiduciary must grant prior written authorization for the compensation and may terminate such compensation upon written advance notification.

Other accounts that may be subject to regulations affecting asset lending transactions include own bank collective investment funds, affiliated mutual funds, and affiliated insurance companies. As part of its account acceptance process, a bank should identify any legal constraints on a customer's ability to participate in the securities lending program.

Tax Considerations

Section 1058 of the U.S. Tax Code provides participants in a securities lending arrangement with relief from recognition of gains and losses on the transfer of securities. Three requirements must be met to obtain this relief:

- The borrower must return securities to the lender that are identical to those borrowed.
- The borrower must, under the terms of the agreement, make payments to the lender that

equal all dividends, interest, and other distributions to which the owner of the securities is entitled during the period the securities are loaned.
- The terms of the agreement cannot reduce the lender's risk of loss or opportunity for gain on the security.

Tax treatment of loaned assets is complex and may affect a lender's holding period and basis in a security. DDs should have qualified tax professionals review their facilitated lending program to ensure that it meets the requirements of the tax code and any Internal Revenue Service regulations.

The tax consequences of digital asset lending are less established than that of securities lending and is an area of ambiguity and possibly forthcoming legal or interpretive changes or guidance. DDs should closely monitor any developments regarding the tax considerations of digital asset lending and seek ongoing guidance from tax professionals, the Internal Revenue Service and state authorities.

Security Interest/Collateral Management

In the context of digital assets in which title does not pass to the borrower, the DD should perfect an appropriate security interest. This may include a security interest under Article 8 of the Uniform Commercial Code. The DD should take all further steps which may be appropriate to strengthen its possession or control and to put in place safeguards to guard against counterparty risk.

If applicable, a DD must ensure that its collateral management process should address risk related to collateral margins, investment of cash collateral, and liquidity. Industry practice is to require collateral in excess of the market value of the assets loaned. Collateral margins may vary by market, and by type of collateral provided. In the United States, cash collateral requirements typically start at 102% of assets borrowed and can significantly increase depending on the nature of the collateral (cash and U.S. securities usually requiring lower ratios) and the volatility and other risk factors associated to the assets being borrowed. The DD's risk management process should address the need for higher collateral margins. If the assets loaned have accrued payments, the collateral margins should be adjusted higher accordingly. The parties generally have the right to negotiate the required collateral margin.

A DD should maintain a robust risk management process to provide ongoing monitoring of its facilitated lending program. Collateral requirements should be based on a holistic assessment of the risks posed by the outstanding asset loans, including:

- The liquidity and volatility of the assets being borrowed; and
- The size of the asset loan and the financial condition of the parties to the transaction;
- Assets, including collateral, involved in a lending program should be marked-to-market. See also *14. Asset Valuation* section.

While the Department does not intend to provide prescriptive guidance for collateral levels for facilitated digital asset loans, beyond the requirement of ensuring full collateralization, the unique and novel risks and uncertainties associated with the digital asset market may justify substantially higher collateral ratios than those typical in more mature and liquid securities markets.

Collateral Margins

The securities loaned and the collateral provided should be marked to market daily and monitored continuously. Typically, when collateral exceeds the required margin, the excess may be returned to the borrower. Alternatively, when the collateral value is less than the required margin, the borrower must provide additional collateral.

The parties will stipulate who is responsible for safekeeping the collateral; the lending agent bank is often selected for this role. Some borrowers may require that the collateral be kept with an independent third party. The party safekeeping the collateral may do that alone, or it may also be responsible for pricing the assets, making margin calls, and collecting income. These responsibilities should be clearly set out in the agency agreement.

Management of Cash Collateral

One of the primary risks a custodian faces in asset lending is managing cash collateral. The investment of cash collateral is the primary source of revenue from securities and digital asset lending activities. The return is typically split between the lending agent (or investment manager) and the lending account. Because of the fee-sharing arrangement, a DD may have an incentive to accept higher risk in managing cash collateral. To control this risk, cash collateral should be invested pursuant to written investment guidelines.

The DD should have a written investment policy addressing management of cash collateral. The policy should establish minimum investment guidelines including permissible types of digital assets or securities, minimum credit quality standards, maturity and duration matching, and liquidity requirements. The board of directors or its designated committee should approve the policy. A lender may wish that the DD use the lender's own guidelines rather than the DD's guidelines. All terms should be clearly specified in the agency agreement.

If several lending customers use the DD's investment policy guidelines, the DD may manage the customers' cash collateral in a pooled account. If a customer has separate, written investment guidelines, the DD should manage that customer's collateral in a segregated account. A DD may manage a combination of segregated and pooled accounts, depending on customer needs.

Liquidity

DDs are exposed to liquidity risk by the short-term nature of most security loans made in the same manner as securities lending transactions. The DD must maintain adequate liquidity in the cash collateral investments to meet the needs of both borrower and lender. The lender has the option of recalling loaned assets at any time (i.e., if they want to sell them). Many borrowers clear lending positions off their books for their periodic accountings. On an overnight basis, borrowers may return large quantities of borrowed securities, only to borrow them again the next day. A DD should have a clearly defined policy restricting the investment of collateral into high-quality liquid assets.

Management of Indirect Financial Risk

The investment guidelines (the DD's or the customer's) provide the framework for managing the interest rate, credit, price, and liquidity risks associated with managing cash collateral. The manner in which the DD manages these risks may affect the DD's own reputation and strategic risk. If applicable, the DD should have a system in place to identify, measure, monitor, and control the risk inherent in managing the cash collateral to ensure that the level of risk present is consistent with customer's directions and the DD's internal risk tolerance. If the DD manages the cash collateral within the established policy guidelines, contractually it should not be liable for losses because of its management of cash collateral. However, in several highly publicized cases involving security custodians in the mid-1990s, banks absorbed significant losses from the management of cash collateral to protect customer relationships and their own reputations.

Rehypothecation Prohibited

Rehypothecation is defined as the "simultaneous reuse or repledging of a digital asset that is already in use or has already been pledged as collateral to another person." Typically, rehypothecation occurs when assets being held as collateral by a lender of an asset repledges those assets as part of a separate financing arrangement. Rehypothecation presents heightened risks in digital asset markets which can be opaque and lack lenders of last resort.

Rehypothecation of securities by prime brokers is regulated by the Federal Reserve Regulation T and SEC Rule 15c3-3, which limit the percentage of client assets that a prime broker may rehypothecate. Rehypothecation presents credit and counterparty risks to the parties involved in the transaction, and broader systemic risks to the financial system. The rehypothecation of client assets are reported to have led to significant problems in the aftermath of the failures of Lehman Brothers and MF Global.

Subject to the DD's own restrictions and per a customer's request, one loan or other transaction of customer digital assets outside of the DD is permissible, including use of the digital asset as collateral for a security interest regarding an unrelated transaction outside of the DD.

The rehypothecation of digital assets legally possessed or controlled in the name of DD customers by the DD is prohibited. DDs should clearly prohibit rehypothecation in their facilitated lending agreements and implement controls to prevent the rehypothecation of assets, including penalties or liquidated damages provisions.

Asset Lending Operations

An efficient and well-organized custody operation system is essential to an asset lending program. A DD must ensure that its systems are capable of handling a large volume of facilitated digital asset loans and ancillary permissible activities. The DD should be willing to devote sufficient resources to technology to support a lending program.

General controls and processes for safekeeping and settlement are common to custody and lending activities. Other operational needs for lending activities that a DD should consider, include:

- Loan scheduling/allocation;
- Mark-to-market program;
- Tracking income, corporate actions, and other governance events for assets on loan;
- Cash collateral management (custodian does not normally invest customer assets);
- When collateral is in the form of securities rather than cash, and there is no DVP mechanism, the common practice is to deliver the collateral 1-2 days prior to borrowing the security. On return, collateral is returned before the security;
- Foreign registration regulations may preclude the redelivery of foreign- registered securities.

Recordkeeping and MIS

Management's ability to manage, monitor, and control risks arising from asset lending activities depends on timely and accurate information.

DDs should have an automated reporting system that should at a minimum provide daily reports of exceptions, assets available for loan, assets on loan, valuation of collateral, daily mark-to-market information, and margin calls.

Allocation of Loans among Lenders

A DD should have a process in place to allocate the loans fairly and equitably among the possible lenders for a particular asset or for single-source lending. The system should be independently tested when adopted or revised and should be retested periodically thereafter. It is not sufficient for a DD to rely on testing performed by the software or system developer.

Regulatory Reporting

Asset lending and borrowing transactions must be reported in accordance with the FFIEC's "Instructions for the Consolidated Reports of Condition and Income."

10.7. Examination Procedures

Procedure	Comments
Selection of Borrowers Objective: Evaluate the DD's due diligence process for borrowers.	
1. Evaluate the DD's due diligence process. Consider whether: • There is a process in place to ensure initial and ongoing borrower reviews. • Borrower risk profiles are developed, including an evaluation of how the borrower typically uses the borrowed assets. • Monitoring processes are in place.	
Loan Agreement with Borrower Objective: Evaluate the DD's borrower loan agreements against best practices	
1. Determine whether the DD's processes ensure that written agreements are in place for all borrowers. Consider whether: • A standard or master agreement is used for all borrowers. • Customized agreements are used and, if so, whether they are reviewed by counsel prior to execution. • The DD's written agreements do not contain any duties, responsibilities, and abilities that constitute more than mere "facilitation" by the DD of a lending transaction, and that they do not allow for the DD to engage in any activity which is not permitted by the NFIA.	
2. Review a sample of agreements to determine whether they address the following: • Transfer of legal title and structure of the transactions or appropriate security interests. • Length of the loans. • Acceptable forms of collateral or security interests. • The frequency of repricing of loaned assets. • If applicable, margin requirements,	

Procedure	Comments
including higher margin requirements for volatile assets. • Margin calls and return of excess collateral. • Assumption of risks by the customer. • Manufactured payments or similar ancillary or subsidiary value including forks, airdrops and staking. • Rebate rates or other fees. • Termination of loans (including recall and time for return). • Applicable disclosures required under Neb. Stat. § 8-3008 • Investment of cash relating to lent assets. • Return of assets identical to those borrowed. • Liens. • Applicable law. • Events of default.	
Agency Agreement with Lending Customers Objective: Evaluate the DD's agreements with lending customers against best practices.	
1. Determine whether written agreements are in place for all customers participating in the facilitated lending program.	
2. Review a sample of the agreements to determine whether they address: • Acceptable forms of collateral and margin requirements or security interests. • Investment of cash collateral, including any lender specified investment guidelines. • Approval of borrowers or any restricted borrowers. • Fees/revenue split. • Indemnification and limitation of liability. • Termination of the loan, including notification requirements for any recalls and time for return. • Liens. • Applicable law.	

Procedure	Comments
• Events of default.	
Legal and Regulatory Requirements Objective: Evaluate the DD's compliance with asset lending regulations.	
1. Determine whether the DD has a process to ensure compliance with: • The requirements of PTE 81-6 and PTE 82-63 covering lending securities for accounts subject to ERISA. • The requirements of the Investment Company Act of 1940 for investment company assets loaned. • Insurance regulations for insurance company assets loaned. • Applicable disclosure requirements under Neb. Stat. § 8-3008. • Other regulated industries.	
Management of Cash Objective: Evaluate the DD's policies and practice for cash management.	
1. Determine whether the process established for the investment of cash is adequate. Consider whether: • The DD has established guidelines that have been approved by the board or an authorized committee. • The lender's investment policy guidelines/restrictions are written, are reviewed/confirmed periodically, and do not conflict with the DD's guidelines unless approved by the board or an authorized committee.	
2. Review the DD's process for monitoring compliance with the applicable investment guidelines for each account or cash pool. Consider whether: • Exceptions are promptly identified and reported (to the investment manager, compliance officer, or a committee). • The process for pricing assets is adequate. • The cash-monitoring process ensures	

Procedure	Comments
that all cash is invested or appropriately safeguarded. • The process for the calculation of returns is adequate.	
Operational Controls The general process for asset movement, dual control, daily reconcilement of transactions, trade processing, and monitoring of aged fails are addressed in previous procedures. The following process reviews relate to operational controls for asset lending activities. Objective: Assess the adequacy of the DD's facilitated lending program's operational controls.	
1. Determine whether the operational control process for lending is adequate. Consider whether: • Assets are marked to market daily, and the updates are forwarded to monitoring personnel. • The DD's process for notifying management of margin calls, collateral returns, time for return or recalls of assets on loan is appropriate. • The DD has a process to monitor invested assets for lenders.	
2. Determine whether the DD has a process for tracking income (manufactured payments and other ancillary and subsidiary value) and corporate actions on loaned assets. Consider whether the DD: • Notifies lending clients of dividend/corporate action items while assets are on loan. • Monitors the receipt of manufactured payments or other ancillary or subsidiary value from borrowers of assets on loan.	
3. Determine whether the DD's process for the allocation of loans is adequate. Consider whether: • The queuing mechanism considers equitable allocation of asset loans between lending accounts or accounts for single-source lending. • The allocation of recalls between borrowers is equitable. • The process allows for any lender	

Procedure	Comments
preferences or restrictions. • The algorithms used in the process are reviewed and independently tested.	
International Asset Lending Although international asset lending is similar to domestic (U.S.) lending, several differences are addressed by the following procedures. Objective: Assess the adequacy of the DD's international asset lending policies and practices.	
1. Determine whether the DD has a process to identify any legal, regulatory, tax, or other requirements of the jurisdictions in which they operate. Consider the adequacy of the DD's process to: • Monitor risk in each jurisdiction.[69] • Monitor restrictions/guidelines on collateral.[70] • Ensure that corporate actions on assets loaned (and returned) are appropriately exercised. • Obtain favorable tax treatment of asset lending transactions (as the bank would using Internal Revenue Code 1058 in the United States.) • Meet local documentation requirements.	
Digital Asset-Specific Lending Considerations Objective: Assess the adequacy of the DD's facilitated digital asset lending program with respect to the unique aspects of digital assets.	
1. What controls does the DD have in place to prevent the rehypothecation of assets? Is this prohibited in lending agreements?	
2. Does the DD have adequate controls in place to monitor for changes in the price of assets and collateral?	

[69] Where there is no DVP mechanism, the common practice is to deliver the collateral one to two days prior to borrowing the security. On return, collateral is returned before the security. Parties are exposed to counterparty credit risk for the amount of the collateral during this time.

[70] In some countries, there may be restrictions on the investment of cash collateral or the type of acceptable collateral.

Procedure	Comments
3. Are the DD's collateral or security interest requirements adequate, and risk-based?	

11. CEA AND CFTC COMPLIANCE CONSIDERATIONS

11.1. Digital Assets Under the Commodity Exchange Act

The Commodity Exchange Act ("CEA") empowers the CFTC to regulate the trading of futures, options, and other derivatives involving commodities. The CEA defines a "commodity" to include "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in."

The CEA requires that entities engaged in the business of facilitating trading and related derivatives to register with the CFTC, subject to certain exemptions. An entity that permits its customers to engage in the purchase or sale of a commodity on a leveraged or financed basis and not resulting in "actual delivery" to customers generally must register with the CFTC as an FCM. These requirements apply to "retail commodity transactions" which are defined to include[71] "any agreement, contract or transaction in any commodity that is (I) entered into with, or offered to (even if not entered into with), a person that is not an eligible contract participant or eligible commercial entity; and (II) entered into, or offered (even if not entered into), on a leveraged or margined basis, or financed by the offeror, the counterparty, or a person acting in concert with the offeror or counterparty on a similar basis."

The CEA also prohibits[72] any person from operating a facility for trading or processing commodity swaps unless the facility is registered as a swap execution facility ("SEF"). The Department does not generally consider a smart contract to constitute a swap. Similarly, the CEA requires that entities that facilitate the trading of futures or option contracts on any underlying commodity to be registered as a designated contract market ("DCM").

Digital assets such as virtual currency typically meet the Commission's definition of commodity. This was established in a 2015 CFTC enforcement order [73] against Coinflip, Inc., a company engaged in bitcoin swap transactions. In the order, the CFTC stated, "[b]itcoin and other virtual currencies are encompassed in the definition [of commodity] and [are] properly defined as commodities". The enforcement order then went on to determine that Coinflip operated a facility for the trading of swaps requiring registration under the CEA but did not register the facility as a Swap Execution Facility as required under Section 5h(a)(1) of the CEA.

The CFTC has issued several announcements with further guidance on specific situations involving digital assets. These are summarized in the table below:

Date	CFTC Guidance or Order	Summary
7/6/2017	In the Matter of the Application of LedgerX LLC for Registration as a Swap Execution Facility	Order granting LedgerX LLC a registration as a swap execution facility.

[71] See 7 U.S.C. § 2(c)(2)(D)(i).
[72] See 7 U.S.C. § 7b-3(a)(1).
[73] Commodity Futures Trading Commission ("CFTC"): Release Number 7231-15.

7/24/2017	In the Matter of the Application of LedgerX, LLC For Registration as a Derivatives Clearing Organization	Order granting LedgerX LLC a registration as a Derivatives Clearing Organization.
10/4/2017	CFTC Primer on Digital Currencies	Overview presentation
12/1/2017	CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange	Statement from CFTC Chairman J. Christopher Giancarlo on the self-certification of bitcoin futures products by CFTC regulated entities including Cantor Exchange and the Chicago Board of Exchange Futures Exchange (CFE).
12/20/2017	CFTC Proposed Interpretation - Virtual Currency and 28 Day Actual Delivery Exemption from FCM Registration	CFTC Proposed Interpretation around the 28 Day Actual Delivery Exemption from FCM Registration.
2/15/2018	CFTC Customer Advisory: Beware Virtual Currency Pump and Dump Schemes	CFTC notice advising customers to avoid pump-and-dump schemes that can occur in thinly traded or new "alternative" virtual currencies and digital coins or tokens.
5/21/2018	CFTC Staff Advisory No. 18-14: Advisory with respect to Virtual Currency Derivative Product Listings	CFTC Staff Advisory to Designated Contract Markets, Swap Execution Facilities, and Derivative Clearing Organizations. The advisory covers (A) enhanced market surveillance; (B) coordination with CFTC staff; (C) large trader reporting; (D) outreach to stakeholders; and (E) DCO risk management.
10/11/2019	CFTC—FinCEN—SEC Joint Statement on Activities Involving Digital Assets	Joint Statement from the leaders of the CFTC, FinCEN and SEC on BSA/AML Compliance related to Digital Assets.
2/18/2020	CFTC Letter; Re: SEC v. Telegram Group, Inc., et al., No. 1:19-cv-09439 (PKC)	Letter from the CFTC to the court overseeing the referenced case discussing if

		a planned digital currency, the "Gram", is a commodity and/or security.
3/24/2020	CFTC Final Interpretive Guidance on Actual Delivery for Digital Assets (28 Day Limitation)	CFTC Final Interpretation around the 28 Day Actual Delivery Exemption from FCM Registration.
10/21/2020	CFTC Letter No. 20-34; Accepting Virtual Currencies from Customers into Segregation	CFTC advisory to FCMs regarding the holding of virtual currency in segregated accounts. The advisory provides guidance to FCMs on how to hold and report certain deposited virtual currency from customers in connection with physically delivered futures contracts or swaps.
12/17/2020	Digital Assets Primer	LabCFTC released a digital assets primer with an overview of digital assets, CFTC regulatory jurisdiction and applicable rules, and topics for further consideration by regulators.
08/23/2021	Statement of Commissioner Dawn D. Stump on the CFTC's Regulatory Authority Applicable to Digital Assets – "Digital Assets: Clarifying CFTC Regulatory Authority & the Fallacy of the Question, 'Is it a Commodity or a Security?'"	Statement from a CFTC Commissioner [74] with 10 key points clarifying CFTC's regulatory authority applicable to digital assets & the legal basis for such. "The CFTC does not regulate commodities…it regulates derivatives".

[74] Not an official statement of the CFTC.

11.2. Actual Delivery, Retail Transactions, and Identified Banking Product Exemption

As discussed above, the CEA requires commodity derivative transactions with the retail[74] public to be traded on CFTC-licensed futures exchanges. This includes commodities transactions that are leveraged through margin or other financing. An exception to this requirement has been adopted in the case of retail transaction in commodities[76] where "actual delivery" of the commodity is made within 28 days of entering the transaction.

The CFTC issued guidance[77] in August 2013 on interpreting the meaning of "actual delivery" in this context. This guidance set out a "functional approach" which is based on the analysis of a list of factors that extend beyond the language used by the parties to the transaction. Certain transactions where title is transferred only by book entry do not qualify as "actual delivery", while "actual delivery" can occur in circumstances when another party takes possession or title of the commodities on the buyer's behalf.

More recently, the CFTC has had to address the interpretation of "actual delivery" in the context of retail transactions involving digital assets. In 2020 the CFTC issued final guidance[78] on the interpretation of "actual delivery" in this context. Under this guidance "actual delivery" of a digital asset has occurred when:

> "(1) a customer securing: (i) possession and control of the entire quantity of the commodity, whether it was purchased on margin, or using leverage, or any other financing arrangement, and (ii) the ability to use the entire quantity of the commodity freely in commerce (away from any particular execution venue) no later than 28 days from the date of the transaction and at all times thereafter; and
>
> (2) the offeror and counterparty seller (including any of their respective affiliates or other persons acting in concert with the offeror or counterparty seller on a similar basis) do not retain any interest in, legal right, or control over any of the commodity purchased on margin, leverage, or other financing arrangement at the expiration of 28 days from the date of the transaction."

The CFTC's guidance also includes the following examples which discuss how the above criteria apply to specific situations:

> Example 1: Actual delivery of virtual currency will have occurred if, within 28 days after entering into an agreement, contract, or transaction, there is a record on the relevant public distributed ledger or blockchain address of the transfer of virtual currency, whereby the entire quantity of the purchased virtual currency, including any portion of the purchase made using leverage, margin, or other financing, is transferred from the counterparty

[75] The "retail public" does not include banks, financial institutions, insurance companies, and investment companies for instance. See CEA Section 1a(18).
[76] CEA Section 2(c)(2)(D)(ii)(III)(aa)
[77] Retail Commodity Transactions Under Commodity Exchange Act, 78 Fed. Reg. 52,426 (Aug. 23, 2013).
[78] "CFTC Issues Final Interpretive Guidance on Actual Delivery for Digital Assets," CFTC (Mar. 24, 2020).

seller's blockchain address [79] to the purchaser's blockchain address, over which the purchaser maintains sole possession and control. When an execution venue or other third-party offeror acts as an intermediary, the virtual currency's public distributed ledger should reflect the purchased virtual currency transferring from the counterparty seller's blockchain address to the third-party offeror's blockchain address and, separately, from the third-party offeror's blockchain address to the purchaser's blockchain address, over which the purchaser maintains sole possession and control.

Example 2: Actual delivery will have occurred if, within 28 days after entering into a transaction: (1) The counterparty seller or offeror has delivered the entire quantity of the virtual currency purchased, including any portion of the purchase made using leverage, margin, or financing, into the possession of a depository[80] (i.e., wallet or other relevant storage system) other than one owned, controlled, operated by, or affiliated with, the counterparty seller (including any parent companies, subsidiaries, partners, agents, affiliates, and others acting in concert with the counterparty seller)[81] that has entered into an agreement with the purchaser to hold virtual currency as agent for the purchaser without regard to any asserted interest of the offeror, the counterparty seller, or persons acting in concert with the offeror or counterparty seller on a similar basis; (2) The purchaser has secured full control over the virtual currency (e.g., the ability to remove as soon as technologically practicable and use freely up to the full amount of purchased commodity from the depository at any time, including by transferring to another depository of the customer's choosing); and (3) With respect to the commodity being delivered, no liens (or other interests or legal rights of the offeror, counterparty seller, or persons acting in concert with the offeror or counterparty seller on a similar basis) resulting or relating to the use of margin, leverage, or financing used to obtain the entire quantity of the commodity delivered will continue after the 28-day period has elapsed[82]. This scenario assumes that no portion

[79] The source of the virtual currency is provided for purposes of this example. However, the focus of this analysis remains on the actions that would constitute actual delivery of the virtual currency to the purchaser.

[80] The offeror may associate with an affiliated depository in Example 2 that the customer chooses to utilize, but such an affiliated depository should be: (i) A ''financial institution'' as defined by CEA section 1a(21); (ii) a separate line of business from the offeror not subject to the offeror's control; (iii) a separate legal entity from the offeror and any offeror execution venue; (iv) predominantly operated for the purpose of providing custodial services for virtual currency and other digital assets; (v) appropriately licensed to conduct such custodial activity in the jurisdiction of the customer; (vi) offering the ability for the customer to utilize and engage in cold storage of the virtual currency; and (vii) contractually authorized by the customer to act as its agent.

[81] The CFTC recognizes that an offeror could act in concert with both the purchaser and the counterparty seller in the ordinary course of business if it intermediates a transaction. This level of association would not preclude the offeror from maintaining an affiliation with a depository in a transaction that otherwise results in actual delivery pursuant to this example. However, pursuant to this example, actual delivery does not occur if the offeror, the offeror's execution venue, or any of its subsidiaries or affiliates, is also the counterparty to the retail commodity transaction at issue.

[82] Although it will consider all relevant factors and circumstances, the CFTC believes that actual delivery would not occur if a lien or similar interest is retained upon the specific virtual currency purchased beyond the 28-day actual delivery period, as such a lien is likely to preclude the customer from using the virtual currency freely as a medium of exchange in commerce. However, the CFTC understands that actual delivery may still occur when liens exist on other collateral, including virtual currency or digital assets other than the specific virtual currency that is the subject of the retail commodity transaction.

of the purchased commodity could be subjected to a forced sale or otherwise removed from the customer's control as a method of satisfying this example.

Example 3: Actual delivery will not have occurred if, within 28 days of entering into a transaction, the full amount of the purchased commodity is not transferred away from a digital account or ledger system owned or operated by, or affiliated with, the offeror or counterparty seller (or their respective execution venues) and received by a separate, independent, appropriately licensed, depository or blockchain address in which the customer maintains possession and control in accordance with Example 2.

Example 4: Actual delivery will not have occurred if, within 28 days of entering into a transaction, a book entry is made by the offeror or counterparty seller purporting to show that delivery of the virtual currency has been made to the customer, but the counterparty seller or offeror has not, in accordance with the methods described in Example 1 or Example 2, actually delivered the entire quantity of the virtual currency purchased, including any portion of the purchase made using leverage, margin, or financing, regardless of whether the agreement, contract, or transaction between the purchaser and offeror or counterparty seller purports to create an enforceable obligation[83] to deliver the commodity to the customer.

Example 5: Actual delivery will not have occurred if, within 28 days of entering into a transaction, the agreement, contract, or transaction for the purchase or sale of virtual currency is rolled, offset against, netted out, or settled in cash or virtual currency (other than the purchased virtual currency) between the customer and the offeror or counterparty seller (or persons acting in concert with the offeror or counterparty seller).

The "actual delivery" guidance for retail commodity transactions may impact a DD in two capacities. Firstly, to the extent that a DD is engaged with a third party which facilitates the sale of commodities on a financed or leveraged basis to DD customers in the retail public without CFTC registration and acting in concert with an offeror or counterparty, the DD must ensure that its third party relies on the actual delivery guidance described above. Secondly, a DD, in its role as a custodian may serve as the depository taking possession/control of digital assets on behalf of customers, as described in the CFTC's Example 2. While the parties to the commodity transaction will likely themselves have obligations, the DD should perform due diligence on these relationships, to ensure their clients are not improperly utilizing the DD's custody services.

Additionally, a further exception to the Commodity Exchange Act exists for "identified banking products."[84] A list of identified banking products is located in *Section 6.3 "Regulation R and Other Registration Exceptions"* of this Manual.

[83] This ''enforceable obligation'' language relates to an element of a separate exception to CEA section 2(c)(2)(D) that is limited by its terms to a commercial transaction involving two commercial entities with a preexisting line of business in the commodity at issue that is separate and distinct from the business of engaging in a retail commodity transaction. See 7 U.S.C. 2(c)(2)(D)(ii)(III)(bb).
[84] 7 U.S.C. § 27a.

11.3. Futures Commission Merchants

Entities which wish to solicit or accept orders to buy or sell futures contracts, options, retail off-exchange contracts or swaps, and accept money or other assets from customers to support such orders must register with the CFTC and the National Futures Association ("NFA") as an FCM. Typically, a banking organization that would like to support its customers in these activities will organize a subsidiary or affiliate which will seek appropriate registration as an FCM.

FCMs are subject to the Commodity Exchange Act, as well as rules and regulations issued by the CFTC, the NFA, and the exchanges or other execution facilities through which they transact.

An FCM may deposit funds or custody assets with DD. This may be a common arrangement for FCM's affiliated with the DD. Examiners should be aware that FCMs have regulatory obligations related to the assets that they might deposit with a DD, particularly requirements to segregate customer funds as described in 17 CFR 1.20, 17 CRF 22.5 and 17 CFR 30.7 These are, however, regulatory requirements on the FCM, and subject to examination by the CFTC and NFA. See, also, the CFTC's Advisory Letter No. 20-34 [85] "Accepting Virtual Currencies from Customers into Segregation".

The OCC has issued a Manual on examining the activities of Futures Commission Merchants affiliated with a national bank[86] which may be useful resource for the Examiner.

[85] Commodity Futures Trading Commission ("CFTC") "Release Number 8291-20" (October 2020).
[86] Office of the Comptroller of the Currency ("OCC") "Futures Commission Merchant Activities" (November 1995).

11.4. Examination Procedure

Procedure	Comments
CEA Compliance Objective: Assess the DD's compliance with the CEA and other CFTC regulations and guidance.	
1. Does the DD's third parties' activities in digital assets or digital asset derivatives require CFTC registration? If so, does the DD ensure that those third parties have a CFTC registration?	
2. If a DD is relying on CEA guidance with regards to transactions facilitated through third parties, evaluate if the transactions and activity are structured to comply with relevant statutory requirements, court cases and CFTC guidance on "actual delivery".	
3. Does the DD hold assets for an FCM? If so, does the DD have in place any procedures to ensure that the FCM is compliant with its requirement to segregate customer assets?	
4. Has the DD received any inquiries from the CFTC related to digital asset activity?	
5. Has the DD received any complaints connected with commodity related activities, including related to possible fraud or market manipulation of digital assets?	
6. Does the DD facilitate transactions through a third party that rely on the CFTC's "actual delivery" guidance? If the DD does, review a sample of transactions for Compliance with the CFTC's guidance.	
7. Does the DD act as a depository for customers who engage in digital asset transactions which rely on the CFTC's "actual delivery" guidance? If the DD does, review a sample of transactions for Compliance with the CFTC's guidance. Does the DD have a due diligence process for reviewing the counterparties, and their compliance practices, that their customers transact with?	

12. PREVENTION OF MARKET MANIPULATION

12.1. Overview

Market or price manipulation is intentional conduct designed to deceive market participants by controlling or artificially affecting the market or perceived market of an asset. Manipulation may involve, among other things, affecting the real or perceived supply or demand for an asset, spreading false or misleading information about the asset or market for the asset, or placing fictious orders or trades. Market manipulation is perhaps most widely associated with the securities markets. However, the same or similar manipulative behaviors present risks to digital asset markets as well. The CEA makes it unlawful[87] for a person to "directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate…" The CEA also makes it unlawful[88] for any person to "directly or indirectly, manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity."

Further, the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act granted the CFTC authority to promulgate and enforce "rules and regulations are reasonably necessary to prohibit trading practice that is disruptive of fair and equitable trading" On July 7, 2011, the CFTC adopted Rule 180, which is modeled on Section 10b-5 of the Securities Exchange Act of 1934, and prohibits "trading on the basis of material nonpublic information in breach of a pre-existing duty (established by another law or rule, agreement, understanding or some other source) and trading on the basis of material nonpublic information that was obtained through fraud or deception."

A DD should maintain policies and conduct appropriate market surveillance to prevent, detect and combat manipulative or otherwise illegal trading practices in traditional and digital asset markets. The NFIA[89] also requires that, "A digital asset depository shall establish and maintain programs for compliance with the federal Bank Secrecy Act, in accordance with 12 C.F.R. 208.63, as the act and rule existed on January 1, 2022."

A DD's market surveillance program, which may be developed internally or through a third-party vendor, should be tailored to the risk profile, considering its businesses, product and service offerings, and clients. A DD should calibrate its market surveillance program to its risk profile by performing periodic risk assessments to identify the risks presented by the DD's products, services, markets, and customers.

[87] 7 U.S.C. § 9(1).
[88] 7 U.S.C. § 9(3).
[89] Neb. Rev. Stat. § 8-3005(5) (LB 707, 2022)

Policies and Procedures

A DD's market surveillance program should be fully documented in policies and procedures. The policies should articulate:

- The structure of the program and key controls.
- The roles and responsibilities of the DD officers or designated supervisors responsible for the program, its oversight and executing key functions within the program.
- Any activities and behaviors the DD have prohibited due to market manipulation risks.
- The process for escalating activities identified as potentially manipulative, unlawful, or otherwise prohibited. The policies should identify both internal escalation paths, as well as articulating the responsibilities for reporting activities to external regulators or law enforcement officials when appropriate. The policies should also ensure that the escalation process is properly documented.

Risk Assessment

The DD's market surveillance program should be calibrated to the risk profile of the DD. This tailoring should be supported by a documented risk assessment. The DD should perform the risk assessment during the design of their initial Market Surveillance program, and then refresh it on a periodic basis thereafter.

The first component of the risk assessment should be an inherent risk analysis. This may consider, among other factors:

- The customer base of the DD. This may include the types of customers (e.g., retail, institutional, corporate), the sophistication and financial resources of the customers, and the customers' potential access to confidential information.
- The products and service that the DD offers, particularly emphasizing the assets that the DD or its customers are active in. For instance, securities, commodities, and digital assets are subject to distinct regulatory requirements and oversight, and present unique market manipulation risks. The DD's inherent risk analysis should identify and prioritize the associated risks specific to the DD's and its customers' activities.
- The characteristics of the markets that the DD or its customers are active in. Manipulative practices may vary drastically between markets. For instance, some manipulative practices are targeted at illiquid markets or assets, while other manipulative practices are design to take advantage of specific electronic order book protocols. The DD's inherent risk analysis should take into account the unique features and risks presented by the markets in which the DD and its customers are active.

The second component of the risk assessment should be a control coverage and effectiveness assessment. This may consider:

- Are identified potential market manipulative risks mitigated by controls?
- Are the controls used to mitigate the risks enough and effective?

The third component of the risk assessment should be a residual risk analysis and action plan. The purpose of this is to identify any risks that, at the time of the risk assessment, are not appropriately managed and to identify an action plan, and timeline, for implementing or revising controls appropriately.

Market Surveillance

A DD must establish a program to monitor market activity that is conducted on its own behalf or by its customers. This is required by the DD even if the customer activities are being conducted or executed at a third party. The level and sophistication of this monitoring should be calibrated to the risk profile of the DD, including the volume and complexity of the transaction flow. An DD involved in minimal market activity, may rely on more manual controls than a DD that is processing, or is party to, a high volume of market activity.

Software vendors offer market monitoring automated software solutions. A DD may choose to use a vendor solution or develop a proprietary system. In either case, the system(s) must be calibrated to detect risks and manipulative behaviors identified as presenting elevated risks through the risk assessment process. Typically, a market surveillance system will monitor market activity against a suite of rules and specific set parameters, specifically designed to detect manipulative behaviors or otherwise anomalous activity. Market surveillance rules typically include thresholds and parameters. The DD should have a documented process for defining these thresholds and parameters and perform periodic calibration to refine them, as well as evaluate the effectiveness of the rules generally. If the DD's customer executed transactions with a third party, the DD should ensure that their systems and processes capture and monitor for customer transactions executed at a third party. This may entail getting direct feeds into the DD's market surveillance systems or receiving market surveillance reports from the third parties.

The DD should have sufficient and appropriately trained resources to review alerts generated by the market surveillance system and take appropriate actions to investigate and escalate identified issues appropriately.

12.2. Standards and Due Diligence for Exchange Partners

A DD will often partner with or direct orders to a digital asset exchange. The exchange may or may not be an affiliated entity of the DD. A DD should engage in due diligence with their exchange partners to ensure that the exchange has an appropriate program in place to monitor for market manipulation. Generally, the DD should evaluate a partner's program using the same criteria set that it would use to build and evaluate their own market manipulation programs.

12.3. Market Manipulation Typologies

Market manipulation can take many forms, and different assets and markets present unique risks. Below we give a summary of some of the more common manipulative behaviors.

Manipulative Transactions

This includes trading, or placing orders to trade, that gives a false or misleading impression of the supply of, or demand for financial products or assets, altering the price to an abnormal or artificial level. Specific typologies include "wash trades" which involves market participants simultaneously buying and selling an asset to create misleading or artificial market activity, "pump and dump" which involves a market participant trying to artificially increase the price in a thinly-traded asset with the intent of trying to sell his position into the inflated market at a profit, and "trash and cash" which involves a market participant trying to profit from a decrease in the price level of an asset after disseminating misleading or negative information to attract the attention of potential sellers. In February 2018, the CFTC has issued a Customer Protection Advisory[90] on "pump and dump" schemes within the digital asset market. Additionally, the CFTC[91] brought an action against Coinbase Inc. for misleading, inaccurate reporting and wash trading.

Distortion and Misleading Behavior

This includes behavior designed to give the false or misleading impression of either the supply of, or demand for, a financial product or asset; or behavior that otherwise distorts the market for the financial product or asset.

Misuse of Information

This includes behavior based on information that is not generally available but would affect a market participant's decision about the terms on which to deal. The use of "insider information" is probably most widely associated with the equities markets, where insiders are prohibited, for instance, from using non-public information about the financial results to trade in the markets. The misuse of information also applies to information about the orders or intentions to buy or sell by other market participants and can occur in most regulated markets. The misuse of information can also apply to the term "front-running", where an asset is traded based on insider knowledge of a future transaction that will affect its price.

As an example, in 2015 the CFTC took enforcement action[92] against an individual who used proprietary information about his employer's proprietary trading in energy commodities to enter orders that matched with his employers to benefit himself. In addition, the individual was accused of using non-public information about his employer's orders to engage in "front running" and,

[90] Commodity Futures Trading Commission ("CFTC") "Release Number 7697-18" (February 2018).
[91] Commodity Futures Trading Commission ("CFTC") "Release Number 8369-21" (March 2021).
[92] CFTC "CFTC Docket No. 16 -02" (December 2015).

ultimately, benefit from the price movements caused by the subsequent execution of his employer's gas and oil futures orders.

Additionally, the U.S. Department of Justice[93] (DOJ) charged its first ever digital asset insider trading scheme on June 1, 2022. The DOJ charged a former employee of a Non-Fungible Token ("NFTs") marketplace, OpenSea, on June 1, 2022, for using insider trading information in NFTs.

Dissemination of False and Misleading Market Information

This includes the communication of information that conveys a false or misleading impression about a financial product or the issuer of a financial product, where the person doing this knows the information to be false or misleading.

As examples, in 2016 the SEC took enforcement action[94] against a Pakistani trader who was accused of profiting from the market activity following a false regulatory filing. In June 2020 the SEC took enforcement action [95] against NAC Foundation, and several associated persons, for offering an unregistered offering called "AML BitCoin" based on false claims about NAC and the "AML BitCoin".

[93] U.S. Department of Justice ("DOJ") "Former Employee of NFT Marketplace Charged in First Ever Digital Asset Insider Trading Scheme" (June 2022).
[94] Securities and Exchange Commission ("SEC") "SEC Prevents Trader's Profits from False Filing" (2016).
[95] SEC "SEC Charges Issuer, CEO, and Lobbyist with Defrauding Investors in AML BitCoin" (2020).

12.4. Examination Procedures

Procedure	Comments
Market Manipulation Surveillance Program Objective: Evaluate the adequacy of the DD's market manipulation surveillance program	
1. Evaluate the DD's market manipulation surveillance program. Evaluate the adequacy of the programs, policies, and procedures.	
2. Does the DD require their exchange partners to have anti-manipulation programs? If so, evaluate if the standards and due diligence applied by the DD to exchange partners are sufficient.	
3. Evaluate whether the DD's market manipulation surveillance program considers surveillance of customer transactions executed with third parties. This may include, but not be limited to, obtaining direct feeds into the DD's systems, or obtaining surveillance reports from third parties.	
4. Has an instance of potential market manipulation been detected by the DD? Evaluate the investigation and resolution process followed in any such cases.	

13. DIGITAL ASSET DUE DILIGENCE AND PERMISSIBILITY

13.1. Overview

As of this writing, there are tens of thousands of digital assets. There is no general regulatory authority with oversight of the issuance of new digital assets. Assets can be established by anyone with the requisite technological know-how, and some digital assets have been established by anonymous parties. Moreover, the current array of digital assets offers a wide array of functionalities and are built on a wide array of technologies.

Not every digital asset will be appropriate for custody and allied services offered by a DD. Moreover, it might well be the case that a digital asset is appropriate for a DD to support with respect to some of its service offerings, but not others. Finally, it might be appropriate for certain digital assets to be appropriate for inclusion in the custody and/or service offerings of one DD but not another, depending on factors such as the resources and profile of the DDs.

A DD seeking a DD charter will submit to the Department as part of its business plan a list of the digital assets that it plans to offer custody services for, as well as a detailed list of other activities (e.g., facilitated asset lending activities) that the DD proposes to support with respect to each proposed digital asset. This plan should include a detailed analysis of the features of the asset, associated risks, and how the DD intends to manage those risks.

The analysis of proposed assets or supported activities by the DD should include the following factors:

- Asset Characteristics and Functionality: There are many types of digital assets. Some assets rely on “proof of work” ledgers and others on “proof stake” ledgers. Some assets have central authorities or an otherwise associated organization to support the asset network. Others do not. Some assets represent claims to underlying assets or on associated parties. Others do not. Some assets are classified as securities under the U.S. securities law. Most are commodities. Others are not. There is substantial competition by digital asset creators to develop new assets with novel properties and functionalities.

  A DD’s analysis of a digital asset should start by a careful and full analysis of the characteristics and functionality of the digital asset under consideration and the risks posed by those functionalities. Additionally, the DD should ensure that the due diligence analysis and conclusion is adequately documented.

- Information Security: The security of digital assets is based on the software and typically decentralized network of digital asset users. The software might in turn rely on cryptographic technologies. Security vulnerabilities to the integrity of the assets may arise from flaws in the underlying technology, the software implementation of the protocol, or more general structural considerations of the network.

A DD should evaluate the information security risks of a digital asset prior to seeking approval to custody or support the asset with other allied services. Digital assets that are newer or less common might pose higher risks of undiscovered vulnerabilities, Conversely, however, a DD should not solely rely on the widespread acceptance of digital assets by others as assurance that the information security risk of an asset has been assessed and deem it acceptable. Pursuant to the NFIA[96], the DD can only provide custody services for digital assets or cryptocurrencies that meet the following criteria:

- "Initially offered for public trade more than six months prior to the date of the custody services; or
- Created or issued by any bank, savings bank, savings, and loan association, or building and loan association organized under the laws of Nebraska or organized under the laws of the United States to do business in Nebraska."

- Compliance: Some assets might pose specific or unique regulatory or compliance issues. DDs and their customers are required to comply with all AML and sanctions laws and regulations while providing custody services for assets and providing allied services. For instance, so-called "privacy coins" are cryptocurrencies that integrate anonymizing techniques as part of their design and that feature blockchains that do not reveal full details of counterparties and transactions. These privacy features might hinder compliance with sanctions or anti-money laundering requirements. The specific compliance risks and challenges presented by an asset should be fully analyzed by the DD prior to extending custody or other value-added services to the asset. DDs should also consider legitimate uses of privacy coins, including IT security/prevention of theft and privacy absent criminal activity for high-net worth investors. DDs should consider AML and sanctions regulations and refer to the *DD Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Assets Control Examination Manual* for additional guidance on the regulatory expectations that should be applied in such an analysis.

  Some digital assets, although not all, meet the definition of a security[97] based on the Howey Test and fall under the regulation of the SEC. DDs should consider if a proposed asset is a security within the definition of the Securities Exchange Act of 1933, and if so, if the asset is and is likely to continue to be required to be compliant with applicable SEC regulations.

- Network Administration and Governance: Some digital assets are completely decentralized. Others are tied to an administering organization. An important example of the latter are certain stablecoins which are supported by an organization that promises to redeem the digital assets for fiat currency or other assets. The analysis of a digital asset should include the organizations associated withs the asset, the role of the organization in administering the asset, and the likelihood of the organization to meet its obligations and comply with relevant laws and regulations.

[96] Neb. Rev. Stat. § 8-3024(1) (LB 707, 2022)
[97] SEC Release No. 81207 "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO" (July 2017).

In addition to an organization's delegated network administration functions, many decentralized digital assets networks will need to address the ongoing maintenance and governance of the network including protocol or code changes to address, among other things, security vulnerabilities. In several cases, network governance frameworks have attempted to reverse large scale thefts. A DD's analysis of a digital asset should include an analysis of the governance mechanisms present in the asset network and risks and or features presented by them.

- Market Characteristics: In addition to the structural characteristics of a digital asset and its security, a DD should evaluate the market for the asset. This should include the market capitalization, distribution of holders, and liquidity of the asset. Assets that are held by a small number of holders, are thinly traded may be illiquid or become illiquid. For instance, illiquid assets may pose particularly elevated risks in asset lending arrangements, and the market characteristics should be included in the analysis of which added value services, such as lending, should be offered for a particular asset.

- Other Available Information and Factors: In addition to the factors listed above, a DD should evaluate other relevant information available about a digital asset as part of its initial assessment. This might include: (1) if other regulatory authorities have approved or denied regulated entities to custody the asset, and (2) any press accounts, regulatory actions, or legal cases involving the asset, allegations of misconduct facilitated by the assets, or involving parties associated with the asset.

13.2. Examination Procedures

Procedure	Comments
Digital Asset Due Diligence Objective: Assess the adequacy of the DDs policies and practices to evaluate the digital assets that they support with their products and services.	
1. Review the policies, procedures, and processes related to the asset acceptance process for compliance with the above principles.	
2. Determine if any new digital assets have been accepted since the last examination. If so, • Were the DD's policies and procedures related to the analysis of the new assets followed? • Does the analysis of these assets consider the factors discussed above? • Does the analysis support the decision to accept the asset and the activities of the DD related to this asset?	
3. Ensure that the DD has an adequate process for ongoing due diligence as well.	
4. Ensure that the DD's due diligence process has been properly documented to adequately reflect the analysis conducted and any conclusion.	

14. ASSET VALUATION

While a DD will hold digital assets off-balance sheet, a DD will be required to ascertain the value of digital assets to support a wide range of DD activities including: (1) providing account statements; (2) meeting its fiduciary obligations for appropriate execution of permissible digital asset transactions; (3) determining when permissible transactions involving digital assets meet regulatory or legal thresholds, such as those related to transaction reporting and AML monitoring; (4) facilitating digital asset loans, monitoring the loans and calculating collateral requirements; and (5) obtaining and monitoring insurance coverage.

A DD shall disclose to the Director, upon request, the methodology and data related to its asset valuation calculations and, if possible, use recognized benchmarks or observable, bona-fide, arms-length market transactions. A DD may provide a summary of its methodology to customers or the public which does not disclose proprietary data. A DD shall exercise due care where the current market value of a digital asset is a conditional element of the transaction being executed. A DD shall ensure adherence to its customer agreement and industry best practices relating to the execution of exchange, derivatives, and lending transactions. A DD shall also disclose in advance the source of the asset valuation to the customer and all signatories of the transaction.

The Department does not prescribe the method of asset valuation beyond this guidance. However, the Department expects that DDs use accepted industry practices designed to accurately ascertain the fair value of the digital assets. "Fair value is the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction in the principal (or most advantageous) market at the measurement date under current market conditions (that is, an exit price) regardless of whether that price is directly observable or estimated using another valuation technique."[98] As described, fair value seeks to align an asset's valuation with the prevailing price that a buyer would be willing to purchase the asset at a given point in time, as best can be ascertained.

Principles that a DD's asset valuation methodology should incorporate include:

- The valuation methodology is intended to ascertain the fair value of the assets, at the time of the valuation.
- The valuation method is the result of a documented, reproducible, and auditable process.
- The valuation method is applied consistently across the DD's activities and processes.
- In the case of assets that have active and liquid markets, asset valuations should closely align to the observable clearing price of market transactions in the same asset.
- The methodology adheres to industry best practices.

The Department expects that the digital assets that a DD custodies or otherwise engages with will typically be actively traded on multiple digital asset exchanges. A DD's asset valuation methodology should rely on current trading and price activity from all (or at least a representative cross-section of) available sources. Data from these sources should be aggregated into a single price

[98] Financial Account Standards Board, Fair Value Measurement (Topic 820); 820-10-35-9A.

using a reasonable methodology aligned to the principles above. The aggregation of pricing data from completed transactions across multiple exchanges using a volume weighted average price ("VWAP") is an approach that is currently in use by digital asset custodians.

Exchange-based trading in digital assets may occur in multiple fiat currencies, as well as between digital asset pairs. While a DD will typically seek to obtain a USD-based valuation of a digital asset, a substantial portion of the trading volume in certain digital assets may not directly involve USD. DDs will need to evaluate and monitor which trading pair data is necessary in designing a valuation methodology that accurately and consistently aligns to the fair value of a given asset. In some cases, "price triangulation" may be necessary to obtain a price using data from two or more trading pairs.

Valuation methodologies are likely to be implemented using automated computer methods, and a DD is expected to perform testing on these methods prior to implementation, as well as after any software or methodological updates. In addition, automated methods that rely on data feeds must implement controls to detect, and have exception processes to handle, erroneous and missing data. Controls should also be in place to appropriately handle any actions designed to be triggered by asset valuations, in the event of potentially anomalous behavior by the valuation algorithm or their input data.

A DD should perform asset valuation at a minimum of once per day. A DD should perform more frequent valuations in cases where fluctuations in prices may trigger actions or responsibilities.

14.1. Examination Procedures

Procedure	Comments
Asset Valuation Objective: Evaluate the asset valuation methodology and practices used by the DD.	
1. Review the policies, procedures, and processes related to asset valuation. Evaluate if the valuation process is: ▪ Designed to ascertain the fair value of the assets, at the time of the valuation. ▪ A documented, reproducible, and auditable process. ▪ Applied consistently across the DD's activities and processes. ▪ Aligned to the observable clearing price of market transactions in the same asset, for assets with liquid markets. ▪ Based on industry best practices, if available.	
2. Review any complaints made by DD customers or counterparties related to the valuation of assets.	

15. INSURANCE

Under Nebraska statute[99], "A digital asset depository shall maintain appropriate insurance or a bond covering the operational risks of the digital asset depository, which shall include coverage for directors' and officers' liability, errors and omissions liability, and information technology infrastructure and activities liability as determined by the director."

The Federal Reserve brought evolving Directors and Officers ("D&O") coverage standards to the attention of banks in Supervisory and Regulation Letter 19-12. This letter advises banks that D&O coverage is an important tool for the recruiting and retention of qualified employees and directors and is, more generally, an important risk mitigation tool. In the SR Letter, the Federal Reserve urges each board member and executive officer to consider the following questions regarding a D&O policy's coverage, specifically when considering renewals and amendments of existing policies:

- What protections do I want from my institution's D&O policy?
- What exclusions exist in my institution's D&O policy?
- Are any of the exclusions new and, if so, how do they change my coverage?
- What is my potential personal financial exposure arising from each policy exclusion?

A DD is not required to obtain FDIC insurance but may do so if available. Even when a DD obtains FDIC insurance, the digital asset holdings of a customer entrusted to a DD for safekeeping are not deposits and will not be covered by FDIC insurance in a loss or failure event. A DD must provide to the Director written verification that assets under custody carry appropriate insurance or other financial protections, as determined by the Director, to cover or mitigate potential loss exposure.

Digital asset insurance coverage should include potential losses from risks such as fraud, theft, operational failures and information security breaches; however, the Department does not require that the custodied assets are fully covered by insurance, and recognizes that there have been capacity issues in the digital asset insurance market. [100] The Department does require that the coverage be appropriate for the DD, considering the value of assets under custody and the risk level associated with the DD's activities. Specific considerations should include:

(1) The insurance coverage limit compared with total assets custodied.
(2) Policy limitations that could result in a significant uninsured loss.
(3) Differing coverage levels for certain activities or custody arrangements (e.g., cold, or hot storage).
(4) The structure of the insurance recovery in the event of an extreme loss event exceeding the policy limits.
(5) The prevailing levels of insurance on custodied digital assets offered by custodians with

[99] Neb. Stat. § 8-3023(5) (LB649,2021)
[100] See CoinDesk article "The Crypto Insurance Market May Total $6 Billion. That's Nowhere Near Enough" (November 2018).

similar business profiles.

A DD should provide a minimum level of loss protection to each customer and should provide current information on the insurance coverage of custodied asset to its customers.

DDs may consider entering arrangements with insurers to offer supplemental coverage to individual customers for a fee. DDs may also consider tiered levels of insurance addressing different activities or custody methods. For instance, given the relative increased security of cold storage, custodians have been able to obtain higher levels of insurance for assets custodied in this manner.

A DD should maintain a summary of its insurance policies, including significant policy exceptions, and an analysis of the factors described above. A DD should also consider that policy exceptions may rely heavily on the actions of the DD and compliance with its own policies and procedures. Maintaining fidelity to laws, regulations, supervisory guidance and the DD's policies and procedures therefore is an important component of ensuring that insurance coverage will be available if needed.

15.1. Examination Procedures

Procedure	Comments
Insurance Objective: Evaluate the DD's insurance coverage against the best practice principles set out by the Department.	
1. Review the DD's insurance coverage and supporting analysis and determine if it is appropriate given the risk profile of the institution. In particular: • Consider the insurance coverage limit compared with total assets custodied. • Consider any policy limitations or exceptions that could result in a significant uninsured loss. • Analyze the extent to which conformity to laws, rules, guidance, and the DD's policies and procedures may affect coverage. • Consider if there are differing coverage levels for certain activities or custody arrangements (e.g., cold, or hot storage). • Consider the structure of the insurance recovery in the event of an extreme loss event exceeding the policy limits. • Consider the prevailing levels of insurance on custodied digital assets offered by custodians with similar business profiles.	

16. CUSTODY & FIDUCIARY SERVICES EXAMINATION PROCEDURES

16.1. General Procedure

These general procedures are intended to assist examiners in determining the adequacy of a DD's policies, procedures, and internal controls regarding custody and fiduciary services risk and risk management. The extent of testing and procedures performed should be based upon the examiner's assessment of risk. This assessment should include consideration of work performed by other regulatory agencies, internal and external auditors and other internal compliance review units, formalized policies and procedures, and the effectiveness of internal controls and management information systems (MIS).

Objective: To determine the scope of the examination of custody services and identify examination activities necessary to achieve the stated objectives.

1. Review the following documents to identify any previously noted problems that require follow-up:

- Previous examination reports.
- Examination conclusion comments.
- Supervisory strategy.
- Follow-up activities.
- Work papers from previous examinations.
- Internal and external audit reports, and if necessary, audit work papers.

2. Prepare and submit the First Day Letter and Request List (refer to Appendix C).

3. Verify the completeness of requested information with the request list.

4. Review the following from the DD:

- Any useful MIS or other information obtained from the DD as part of the ongoing supervision process, including but not limited to, applicable written policies and procedures.
- Any useful information obtained from the review of applicable board and committee minutes.
- A list of board and executive or senior management committees that supervise custody and fiduciary services, including a list of members and meeting schedules. Also obtain the name and phone number of the person who maintains copies of minutes.
- Reports related to custody and fiduciary services that have been furnished to any applicable committee or to the board of directors.

5. Determine, during early discussions with management, whether there have been:

- Any significant changes in policies, procedures, computer systems, or personnel relating to custody and fiduciary activities or processes.
- Material changes in products, volumes, or market focus. Review to ensure that the DD's business activities match the permissible activities the DD was approved for by the Director.
- Significant levels and trends for exceptions, fails, or losses for each custody and fiduciary services area.

6. Review the DD's business and strategic plans and determine whether management's plans for the department are clear and reflect the current direction of the department.
7. Using what you learned from these procedures and from pre-exam discussions with DD management, determine the scope of this examination and its objectives.
8. Determine if the DD has trust or fiduciary operations significant enough to warrant a UITRS rating. Refer to the Fiduciary Services Examination Procedures.

16.2. Conclusions

Objective: To communicate findings and initiate corrective action when policies, practices, procedures, objectives, or internal controls are deficient or when violations of law, rulings, or regulations have been noted in the DD's administration of its custody services activities.

1. Compile a brief written conclusion regarding:

- The adequacy of risk management systems, including policies, processes, personnel, and control systems.
- Internal control deficiencies or exceptions.
- DD conformance with established policies and procedures.
- Significant violations of laws, rules, or regulations.
- Corrective action recommended for identified deficiencies.
- The adequacy of MIS.
- Quantity of risk and quality of risk management associatedwith custody services.
- The overall level of compliance with applicable law, accepted industry standards, and DD policies and procedures, to assist in determining the compliance rating.
- Other matters of significance.

2. Identify significant risks. Assess the impact of custody and fiduciary services on the DD's aggregate risks and the direction of those risks.

- Risk Categories: Operational, Liquidity, Market, Reputation, Compliance, Credit, or Strategic.
- Risk Conclusions: High, Moderate, or Low.
- Risk Direction: Increasing, Stable, or Decreasing.

3. Complete the Examination Program Template included in Appendix A.

4. [If applicable] Determine and document the appropriate fiduciary composite and management ratings using the factors listed in the UITRS and the findings from the other fiduciary examination activities.

5. Determine whether the risks identified are of enough significance to bring them to the board's attention in the report of examination. If so, prepare items for inclusion in "Matters Requiring Attention" (MRA).

- The MRA should cover practices that:
  - Deviate from sound principles and may result in potential financial liability if not resolved.
  - Result in substantive noncompliance with laws.
- An MRA should discuss:
  - Causes of the problem.
  - Consequences of inaction.
  - Management's commitment to corrective action.
  - The time frame and person(s) responsible for corrective action.

6. Discuss findings with DD management, addressing:

- Adequacy of risk management systems, including policies, processes, personnel, and control systems.
- Violations of law, rulings, regulations, or significant internal control deficiencies, emphasizing their causes and the potential for risks associated with custody service activities.
- Recommended corrective action for deficiencies cited.
- DD's commitment to specific actions for correcting deficiencies.

7. As appropriate, prepare a brief comment on custody and fiduciary services for the report of examination. In general terms, address the following subjects:

- Quantity of risk.
- Quality of risk management.

8. Prepare a memorandum or update the work program with any information that will facilitate future examinations.

9. Organize and reference work papers in accordance with the Department's guidance. Work papers should clearly and adequately support the conclusions reached.

APPENDIX A: Examination Program Template

Digital Asset Depository Institution Name:
Department Examiner:
Preparer:

Section 1. Business Profile

Products, Services, and/or Function

Organizational Structure

Risk Management Systems

- Supervision
- Policies
- Processes
- Personnel
- Control and monitoring systems
  - ☐ Committees
  - ☐ Risk management function
  - ☐ Compliance program
  - ☐ Self-assessment program
  - ☐ Management information reporting systems
  - ☐ Audit program

Technology and Information Systems

Financial Performance

Section 2. Risk Assessment Profile

I. Risk Assessment System

Risk	Quantity	Quality	Aggregate	Direction
Operational Risk				
Liquidity Risk				
Market Risk				
Compliance Risk				
Credit Risk				
Strategic Risk				
Reputation Risk				

Provide comments addressing the quantity of risk, quality of risk management, aggregate risk, and direction of risk for each category affected by asset management activities. Include a list of key issues and the status of correction action, if applicable. Examiners should refer to the *OCC Handbook for Community Bank Supervision*[101].

Operational Risk

Liquidity Risk

Market Risk

Compliance Risk

Credit Risk

Strategic Risk

Reputation Risk

[101] OCC Handbook for Community Bank Supervision (June 2018)

Include other risks, if appropriate.

II. CAMELS

Provide comments that address the impact of asset management risks and risk management systems on the interagency rating system.
Composite

- Capital
- Asset Quality
- Management
- Earnings
- Liquidity
- Sensitivity to Market Risk

III. Uniform Interagency Trust Rating System

	1	2	3	4	5
Management	☐	☐	☐	☐	☐
Operations, Internal Controls, and Auditing	☐	☐	☐	☐	☐
Earnings	☐	☐	☐	☐	☐
Compliance	☐	☐	☐	☐	☐
Asset Management	☐	☐	☐	☐	☐
Composite Rating	☐	☐	☐	☐	☐

Section 3. Supervisory Strategy

I. Supervisory Cycle:

II. Objectives:

III. Activities:

IV. Work Plans:

APPENDIX B: Uniform Interagency Trust Rating System

The Uniform Interagency Trust Rating System (UITRS) was adopted in 1978 and revised in 1998.[102] The UITRS considers certain managerial, operational, financial, and compliance factors that are common to all institutions with fiduciary activities. Under this system, the supervisory agencies endeavor to ensure that all institutions with fiduciary activities are evaluated in a comprehensive and uniform manner, and that supervisory attention is appropriately focused on those institutions exhibiting weaknesses in their fiduciary operations.

Overview

Under the UITRS,[103] the fiduciary activities of financial institutions are assigned a composite rating based on an evaluation and rating of five essential components of an institution's fiduciary activities. These components are the capability of management; the adequacy of operations, controls, and audits; the quality and level of earnings; compliance with governing instruments, applicable law (including self-dealing and conflicts of interest laws and regulations), and sound fiduciary principles; and the management of fiduciary assets.

Composite and component ratings are based on a scale of 1 to 5. A1 is the highest rating; it indicates the strongest performance and risk management practices and the lowest degree of supervisory concern. A5 is the lowest rating; it indicates the weakest performance and risk management practices and the highest degree of supervisory concern. Evaluation of the composite and component ratings considers the size and sophistication, the nature and complexity, and the risk profile of the institution's fiduciary activities.

The composite rating generally bears a close relationship to the component ratings assigned, but the composite rating is not derived by computing an arithmetic average of the component ratings. Each component rating is based on a qualitative analysis of the factors comprising that component and its interrelationship with the other components. When examiners assign a composite rating, some components may be given more weight than others depending on the situation at the institution. In general, assignment of a composite rating may incorporate any factor that bears significantly on the overall administration of the financial institution's fiduciary activities. Assigned composite and component ratings are disclosed to the institution's board and senior management.

Management's ability to respond to changing circumstances and to address the risks that may arise from changing business conditions, or the initiation of new fiduciary activities or products, is an important factor in evaluating an institution's overall fiduciary risk profile and the level of supervisory attention warranted. For this reason, the management component is given special consideration when examiners assign a composite rating. Management's ability to identify, measure, monitor, and control the risks of its fiduciary operations is also taken into account when assigning each component rating. Appropriate management practices may vary considerably among financial institutions, depending on the size, complexity, and risk profiles of their fiduciary activities. For less complex institutions engaged solely in traditional fiduciary activities and whose directors and senior managers are actively involved in the oversight and management of day-to-day operations, relatively basic management systems and controls may be adequate. At more

[102] For additional reference materials, see the OCC Custody Services booklet as part of the *Comptroller's Handbook* as well as the FDIC Trust Examination Manual, which includes additional examination aids.

[103] Excerpt is from 63 Fed. Reg. 54704-54711, "Uniform Interagency Trust Rating System."

complex institutions, detailed and formal management systems and controls are needed to address a broader range of activities and to provide senior managers and directors with the information they need to supervise day-to-day activities. All institutions are expected to properly manage their risks. For less complex institutions engaging in less risky activities, detailed or highly formalized management systems and controls are not required to receive strong or satisfactory component or composite ratings. The following two sections contain the composite rating definitions and the descriptions and definitions for the five component ratings.

UITRS Composite Ratings

Composite ratings are based on an evaluation of how an institution conducts its fiduciary activities. The review encompasses the capability of management, the soundness of policies and practices, the quality of service rendered to the public, and the effect of fiduciary activities on the institution's soundness. The five key components used to assess an institution's fiduciary activities are the

- capability of management.
- adequacy of operations, controls, and audits.
- quality and level of earnings.
- compliance with governing instruments, applicable laws, and regulations (including self-dealing and conflicts of interest laws and regulations), and sound fiduciary principles.
- management of fiduciary assets.

UITRS Composite Ratings

1	Administration of fiduciary activities is sound in every respect. Generally, all components are rated 1 or 2. Any weaknesses are minor and can be handled in a routine manner by management. The institution is in substantial compliance with fiduciary laws and regulations. Risk management practices are strong relative to the size, complexity, and risk profile of the institution's fiduciary activities. Fiduciary activities are conducted in accordance with sound fiduciary principles and give no cause for supervisory concern.
2	Administration of fiduciary activities is fundamentally sound. Generally, no component rating should be more severe than 3. Only moderate weaknesses are present and are well within management's capabilities and willingness to correct. Fiduciary activities are conducted in substantial compliance with laws and regulations. Overall risk management practices are satisfactory relative to the institution's size, complexity, and risk profile. There are no material supervisory concerns and, as a result, the supervisory response is informal and limited.
3	Administration of fiduciary activities exhibits some degree of supervisory concern in one or more of the component areas. A combination of weaknesses exists that may range from moderate to severe; however, the magnitude of the deficiencies generally does not cause a component to be rated more severely than 4. Management may lack the ability or willingness to effectively address weaknesses within appropriate time frames. Additionally, fiduciary activities may reveal some significant noncompliance with laws and regulations. Risk management practices may be less than satisfactory relative to the institution's size, complexity, and risk profile. While problems of relative significance may exist, they are not of such importance as to pose a threat to the trust beneficiaries generally, or to the soundness of the institution. The institution's

	fiduciary activities require more than normal supervision and may include formal or informal enforcement actions.
4	Fiduciary activities generally exhibit unsafe and unsound practices or conditions, resulting in unsatisfactory performance. The problems range from severe to critically deficient and may be centered on inexperienced or inattentive management, weak or dangerous operating practices, or an accumulation of unsatisfactory features of lesser importance. The weaknesses and problems are not being satisfactorily addressed or resolved by the board and management. There may be significant noncompliance with laws and regulations. Risk management practices are generally unacceptable relative to the size, complexity, and risk profile of fiduciary activities. These problems pose a threat to the account beneficiaries generally and, if left unchecked, could evolve into conditions that could cause significant losses to the institution and ultimately undermine the public confidence in the institution. Close supervisory attention is required, which means, in most cases, formal enforcement action is necessary to address the problems.
5	Fiduciary activities are conducted in an extremely unsafe and unsound manner. Administration of fiduciary activities is critically deficient in numerous major respects, with problems resulting from incompetent or neglectful administration, flagrant or repeated disregard for laws and regulations, or a willful departure from sound fiduciary principles and practices. The volume and severity of problems are beyond management's ability or willingness to control or correct. Such conditions evidence a flagrant disregard for the interests of the beneficiaries and may pose a serious threat to the soundness of the institution. Continuous close supervisory attention is warranted and may include termination of the institution's fiduciary activities.

APPENDIX C: List of Digital Asset Guidance and Supervision Documents from Other Jurisdictions

A number of supervisory bodies have developed regulations, supervisory guidance, and other descriptions of digital assets addressing custody, fiduciary, and more general considerations. Recognizing that supervision of digital assets is an evolving space, the Department highlights a select set of jurisdictional guidance as additional reference points for supervisory and control framework considerations.

Note that this appendix includes an "as of date" of June 30, 2022, and will be updated periodically.

Source	Reference Material
Applicable U.S. federal and state standards for reference	• OCC Custody Services Handbook • OCC Unique and Hard-to-Value Assets Manual • OCC Interpretive Letter #1170 • OCC Interpretive Letter #1174 • OCC Interpretive Letter #1179 • SEC/FINRA Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities • SEC Statement "Custody of Digital Assets Securities by Special Purpose Broker-Dealers" • SEC Staff Accounting Bulletin No. 121 • CFTC's Retail Commodity Transactions Involving Certain Digital Assets • NYDFS Part 200 (Virtual Currencies), particularly Section 200.9 Custody and protection of customer assets
Select Foreign-jurisdiction standards	• Monetary Authority of Singapore – May 2020: Consultation Paper on Proposed Regulatory Approach for Derivatives Contracts on Payment Tokens • Bermuda Monetary Authority Digital Asset Custody Code of Practice • Abu Dhabi's Financial Services Regulatory Authority Guidance – Regulation of Virtual Asset Activities in ADGM • United Kingdom Financial Conduct Authority Custody Rules • Switzerland CMTA Digital Assets Custody Standard
Industry Guidance	• Financial Stability Board Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements • European Parliament Crypto-assets: Key developments, regulatory concerns and responses • Global Digital Finance Code of Conduct Part IX(i) - Principles for Custody "Custodial Wallets"

- Global Digital Finance Crypto Asset Safekeeping and Custody Key Considerations and Takeaways
- Public Company Accounting Oversight Board Audits Involving Cryptoassets
- Switzerland CMTA Digital Assets Custody Standard
- Standard Board for Alternative Investments (SBAI) Operational Due Diligence on Crypto Assets

APPENDIX D: DD Request Letter

As part of the examination planning process, the examiner should prepare a request letter. The list below includes materials that examiners *may* request or request access to for a DD custody and fiduciary examination. This list should be tailored for the specific DD's risk profile and the planned examination scope. Additional materials may be requested as needed.

1.1. Sample First-Day Letter Text

<<NAME OF INSTITUTION>>
<<DATE OF EXAMINATION>>
<<PRIOR EXAMINATION DATE>>
EXAMINER-IN-CHARGE

THE FOLLOWING ITEMS OR MATERIALS ARE REQUESTED TO EXPEDITE THE EXAMINATION OF YOUR INSTITUTION'S CUSTODY AND FIDUCIARY ACTIVITIES.

THE ACCURACY AND TIMELINES OF DATA PROVIDED ARE VITAL TO THE SUCCESSFUL EXAMINATION OF YOUR INSTITUTION. PLEASE HAVE THE FOLLOWING AVAILABLE ON <<DATE>>.

Please provide the following information as of (Insert Date).

If information requested is not applicable, please indicate with a NA.

Requested Items:
<<Insert List>>

1.2. Sample First-Day Letter Request Items

Risk Management

- Make available policies and procedures related to the risk management of custody and fiduciary activities.
- Make available the Minutes of the Board of Directors, trust committee(s) and digital asset committee (if applicable) pertaining since (Insert Date).
- Provide a listing of outside service providers and have copies of their contracts available for review. Examples include software service providers, pricing services, record keepers, proxy voting services, digital asset business service providers and so on.
- Provide the date of the most recent business resumption (contingency) plan and the results of the last contingency plan test.

Personnel

- Make available organization charts showing the reporting structure of key DD staff, and

the job descriptions of key positions.
- Make available the resumes of individuals holding key DD positions.

Operations and Audit
- Make available reports of internal or external Auditors, including any associated action plans or management responses.
- Make available management responses and actions plans prepared to address internal audit reports.
- Make available minutes of the DD's audit committee.
- Make available the results of quarterly audits of the DD's transaction activity, and any resulting corrective action plans.
- Provide the most recent reconcilement(s) and supporting documentation of the department's:

a) demand deposit account(s);
b) safekeeping and/or safekeeping exception report;
c) custody accounts;
d) fiduciary accounts;
e) brokerage accounts;
f) suspense accounts;
g) house accounts; and
h) failed trades.

Regulatory and Legal Matters
- Current statement of assets and liabilities.
- Information on pending matters describing any threatened and/or pending litigation against the DD in connection with its custody or fiduciary activities. Please include the following information:

a) identification of accounts concerned;
b) nature of, or basis for, the litigation;
c) amount involved;
d) present status of the action; and
e) statement as to the probable outcome of the action, together with its cost to the DD.
- Indicate if legal counsel is retained on an ongoing basis to advise the Board of Directors, or management on legal matters pertaining to custody or fiduciary administration.
- Indicate if written legal opinions are obtained and filed in connection with legal questions arising during the course of an account's administration.
- Provide a copy of any communication with state regulators, the Department of Labor, Securities and Exchange Commission, the Federal Reserve, Internal Revenue Service, Commodities and Futures Trading Commission, or Financial Industry Regulatory Authority for the DD, its subsidiaries or affiliates since the previous examination.
- Provide a copy of the customer complaint log since the last examination. If a complaint log is not maintained, provide a list of customer complaints filed since the last examination including the following information:

a) name of complainant;
b) date of complaint;
c) description of the complaint; and

d) resolution of the complaint.

Organization

- Provide an organization chart of the DD.
- Provide a copy of the DD's current strategic plan, marketing plan, and budget.
- Provide a list of all DD subsidiaries and affiliates, together with a brief synopsis of capitalization and activities engaged in by the subsidiary or affiliate.
- Provide information on any acquisitions or mergers since the last examination.
- Provide a list of board and management committees including: (1) the name and function of the committee; (2) the name of committee members; (3) titles of internal committee members and the principal business interest or occupation of external member; (4) annual fees paid, if any.
- Provide the names, titles, and resumes of the DD's principal officers.
- A list of principal DD officers hired since the last examination.
- Provide a list of insurance policies and coverage summaries for principal DD operations, including trust and custody activities.

General Account Administration

- Provide a copy of the DD's privacy policy and customer disclosures.
- Provide a copy of the DD's current strategic plan, marketing plan, and budget.
- Provide a list of DD assets (indicate par and market values of each security):

a) pledged with state authorities;
b) pledged with the trust department; or
c) otherwise segregated and earmarked to secure trust activities or uninvested trust cash.

Custodial Services

- Make available copies of customer custody agreements.
- Make available policies and procedures to ensure the appropriate execution of customer transactions.
- Make available sample documentation evidence the approval or rejection of transactions, and the reasoning or evidence used to support or reject the transactions.
- Make available procedures to analyze and evaluate transactions are executed in accordance with execution practices, and the results of any such analyses.
- Make available any sub-custody agreements.

Fiduciary and Trust Services

- Make available copies of customer trust agreements.
- Make available copies of retirement plan agreements which the DD administers in a fiduciary capacity.
- Provide copies of the last year-end Call Report and the work papers for the preparation of Schedule RC-T. If the institution files Schedule RC-T data on a quarterly basis, also provide the last quarter's Call Report and the work papers for the preparation of Schedule RC-T.
- Provide a copy of the DD's privacy policy and customer disclosures.
- Provide a list of all accounts (e.g., account trial balance), listing for each (note: for items f, g and h please identify if shown at "book" or "market" value):

a) account title and number;

b) account officer;
c) investment officer;
d) principal cash;
e) income cash;
f) invested principal (summary total per account, not detail of assets or tax lots unless requested);
g) invested income (summary total per account, not detail of asset or tax lots unless requested); and
h) summary totals for cash and assets of all accounts (by major appointment category).

- Provide a summary listing of assets by type and CUSIP number and the aggregate number of units held. The report should also provide the total "book" and "market" value of each asset.
- Provide a list of liabilities within accounts, such as borrowings, etc. Please indicate the dollar value of assets pledged by the account, if any, to collateralize such liabilities.
- Provide a list of terminated accounts that have not been distributed, including the reasons therefore.
- Provide a list of watch-listed accounts.
- provide summary information on the following trust activities, if applicable

a) electronic banking, including the use of web sites. Please provide web site addresses, if any.
b) new trust products developed since last examination.

Staking

- Make available copies of customer asset staking agreements.
- Make available copies of asset staking agreements with counterparties and non-customers.

Asset Borrowing

- Make available copies of customer asset borrowing agreements.
- Make available copies of asset borrowing agreements with lenders, counterparties, and non-customers.

Asset Lending

- Make available copies of customer asset lending agreements.
- Make available copies of asset lending agreements with borrowers, counterparties, and non-customers.

Record Keeping

- Make available policies and procedures explaining the recordkeeping practices for transaction activity.

Key Management

- Make available policies and procedures explaining the key management procedures used by the DD, including protocols for segregations of duties.
- Make available any audits or reviews of the key management function.

APPENDIX E. Abbreviations and Key Terms

Abbreviation or Term	Full Name or Description
Airdrop	An airdrop is a distribution of a digital assets, usually for free, to numerous wallet addresses, sometimes in proportion to one's holding in another digital asset.
AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CEA	Commodity Exchange Act
CFTC	Commodities and Futures Trading Commission
CFR	Code of Federal Regulations
CIP	Customer Identification Program
Controllable Electronic Borrowing	The act of receiving digital assets or the use of digital assets from a lender in exchange for the payment to the lender of digital assets, interest, fees, or rewards.
Controllable Electronic Record	An electronic record that can be subjected to control. The term has the same meaning as digital asset and does not include electronic chattel paper, electronic documents, investment property, and transferable records under the Uniform Electronic Transactions Act.
Controllable Electronic Record Exchange	A business that allows customers to purchase, sell, convert, send, receive, or trade digital assets for other digital assets.
Controllable Electronic Record Lending	The act of providing digital assets to a borrower in exchange for digital assets, interest, fees, or rewards.
Controllable Electronic Record Staking	The act of pledging a digital asset or token with an expectation of gaining digital assets, interest, fees, or other rewards on such act
CSD	Central Security Depository
CTR	Currency Transaction Report
Custody Rule	A rule adopted by the SEC under the Investment Advisers Act of 1940 that requires investment advisers to maintain assets with a qualified custodian.
D&O	Director and Officer's Insurance
DD	Digital Asset Depository Institution
Department	Department of Banking and Finance

Digital Asset[104]	Refers to all central bank digital currency, regardless of the technology used, and to other representations of value, financial assets, and instruments, or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology. For example, digital assets include cryptocurrencies, stablecoins, and central bank digital currency. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, or through peer-to-peer technologies.
Digital Asset Depository Institution	A corporation operating a digital asset depository business organized and chartered pursuant to the Nebraska Financial Innovation Act;
Director	Director of Banking and Finance
DK	Don't Know
DOL	Department of Labor
DPoS	Delegated Proof of Stake
EDD	Enhanced Due Diligence
The Exchange Act	Securities Exchange Act of 1934
FINRA	Financial Industry Regulatory Authority
FATF	Financial Action Task Force on Money Laundering
FAQ	Frequently Asked Question
FCM	Futures Commission Merchant
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
Fork	A change to the protocol of a blockchain network
Hard fork	Changes to the blockchain software that renders the new version of the blockchain software incompatible with the previous version of the software.
Honey Pots	Large accumulations of digital assets that might be the target for theft.

[104] Definition from the President's Executive Order "Executive Order on Ensuring Responsible Development of Digital Assets" (March 2022)

HSM	Hardware Security Module
IAA	Investment Advisers Act
ICA	Investment Company Act of 1940
KYC	Know Your Customer
Manufactured payments	Payments made by the borrower of an asset to the lender to mimic the benefits of economic ownership of the borrowed asset, such as staking or dividend payments for equity securities.
ML/TF	Money Laundering / Terrorist Financing
MIS	Management Information Systems
Multisig	Multi-signature or Multi-signature scheme
NFA	National Futures Association
NFIA	Nebraska Financial Innovation Act
NOBO	Non-Objecting Beneficial Owners
NSCC	National Securities Clearing Corporation
OBO	Objecting Beneficial Owners
OFAC	Office of Foreign Assets Control
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
Off-chain	A transaction that is not recorded on a digital asset blockchain or ledger
On-ledger	A transaction that is recorded on a digital asset blockchain or ledger.
Proof of stake	A consensus mechanism to validate assets on a blockchain, that is sometimes configured to provide rewards for participating digital asset holders.
Proof of Work[105]	Means the use of a consensus algorithm in a block-chain network used to confirm and produce new blocks to the chain to validate a cryptocurrency transaction, where competitors complete new blocks and where the algorithm changes the complexity of the competition in a manner that is designed to and/or results in increased energy usage for each competitor when the complexity is increased.
Qualified Custodian	A custodian that meets certain requirements that permit it to custody assets for investment advisers under the Investment Advisers Act of 1940.
SAB	Staff Accounting Bulletin
SEC	Securities and Exchange Commission
SIDD	Separately identifiable department or division

[105] Definition from NY State Assembly Bill A7389C

Soft fork	Changes to the blockchain software that do not render the updated software incompatible with previous versions
Slashing	Penalties for noncompliance with staking protocols.
Stablecoin	A cryptocurrency designed to have a stable value that is backed by a reserve asset.
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

[i]